Institut für Europarecht
Institut de droit européen

Zu den datenschutzrechtlichen Vorgaben für Errichtung und Betrieb von Informationssystemen

Unter besonderer Berücksichtigung der Bearbeitung besonders schützenswerter Personendaten und der Zugriffsberechtigung und am Beispiel des Klienten-Informationssystems für Sozialarbeit (KiSS)

Prof. Dr. *Astrid Epiney*
MLaw *Tobias Fasnacht*

Dieser Beitrag wurde erstmals wie folgt veröffentlicht:
***Astrid Epiney/Tobias Fasnacht,* Zu den datenschutzrechtlichen Vorgaben für Errichtung und Betrieb von Informationssystemen, Jusletter v. 24.2.2014. Es ist möglich, dass die Jusletter-Publikation – die allein zitierfähig ist – im Verhältnis zu diesem Manuskript geringfügige Modifikationen enthält.**

Freiburg, November 2013

Inhaltsverzeichnis

A. Problemstellung

Einrichtung und Betrieb von **computergestützten Informationssystemen**, die **Personendaten** enthalten, werfen regelmässig datenschutzrechtliche Fragen auf, wobei diese grundsätzlich alle datenschutzrechtlichen Prinzipien betreffen (können).[1] Von besonderer Bedeutung ist hierbei regelmässig die Frage des Kreises der **Zugriffsberechtigten**, eine Problematik, die sich dann noch in besonderer Weise stellt, wenn in dem betreffenden Informationssystem **besonders schützenswerte Personendaten** bearbeitet werden. Dabei kann sich die Frage des Zugangs sowohl verwaltungsintern bzw. innerhalb der das Informationssystem betreibenden Stelle oder Behörde als auch in Bezug auf externe Stellen, seien dies nun andere Verwaltungsbehörden oder Private, stellen.

Bei der Beantwortung der Frage nach dem (zulässigen) Kreis der Zugriffsberechtigten – soweit die Datenbearbeitung durch öffentliche Stellen betroffen ist, auf die sich diese Studie beschränkt – kennt das Datenschutzrecht (sowohl auf Bundes- als auch auf Kantonsebene) einerseits Anforderungen an die **gesetzliche Grundlage** (wie bei jeder Datenbearbeitung), andererseits auch solche an die **materielle Ausgestaltung der Zugriffsberechtigungen**, in deren Rahmen die allgemeinen **datenschutzrechtlichen Grundsätze** zu beachten sind. Bei letzteren spielen diejenigen der **Zweckbindung** und der **Verhältnismässigkeit** eine besondere Rolle, Grundsätze, die sich letztlich bereits aus Art. 8 EMRK und Art. 13 BV ergeben und insoweit nicht zur Disposition des Gesetz- oder Verordnungsgebers stehen.[2]

---

[1] Vgl. zur Problematik, mit historischem Bezug, z.B. *Zehnder*, in: Von der Lochkarte zum Mobile Computing, 147 ff.; ausführlich *Bondallaz*, La protection des personnes et de leurs données, 8 ff.; s. auch die Einführung in die datenschutzrechtliche Problemstellungen bei *Belser*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 1, Rn. 8 ff.

[2] Insofern sind die in Art. 4 DSG und Art. 5 KDSG erwähnten Datenschutzgrundsätze auch bei der Erarbeitung spezialgesetzlicher Grundlagen zu beachten, was nach dem Gesagten nicht auf dem Charakter der Datenschutzgesetze als „Supergesetze" (s. diesen Ausdruck bei *Gächter/Egli*, Jusletter v. 6.9.2010, Rn. 270 ff.) beruht, sondern darauf zurückzuführen ist, dass diese Grundsätze letztlich Ausfluss der grund- und menschenrechtlichen Vorgaben sind und diese lediglich ausformulieren. S. insoweit schon *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 2 ff., 7 ff.; *Epiney*, in: Verwaltungsorganisationsrecht, 5 (15 f.); nicht ganz klar in dieser Hinsicht aber teilweise die Rechtsprechung, vgl. BGE 124 I 176 E. 5c; BGE 133 V

Im Folgenden soll vor diesem Hintergrund der Frage nachgegangen werden, welche rechtlichen **Anforderungen an die Errichtung und den Betrieb von Informationssystemen aus datenschutzrechtlicher Sicht** bestehen. Dabei wird besonderes Augenmerk auf die Frage des Kreises der **Zugriffsberechtigten** im Falle der Bearbeitung **besonders schützenswerter Personendaten** gelegt. Im Bestreben, diese Anforderungen an einem konkreten Beispiel aufzuzeigen, soll dabei an das sog. **Klienten-Informationssystem für Sozialarbeit (KiSS)** angeknüpft werden, das von kommunalen und kantonalen Behörden in der Schweiz teilweise – allerdings in unterschiedlicher Ausgestaltung – verwendet wird. In diesem System werden zu Handen von im Sozialwesen tätigen Behörden Informationen der „Klienten" zur Verfügung gestellt, dies letztlich im Hinblick auf die Wahrnehmung der gesetzlichen Aufgaben der involvierten Behörden. Deutlich wird damit auch, dass hier in der Regel das kantonale Datenschutzrecht zur Anwendung kommt, da es um Datenbearbeitungen kantonaler Behörden geht.[3] Daher wird in dieser Studie beispielhaft auf die Rechtslage im Kanton Bern und damit das Berner Datenschutzgesetz abgestellt.

Damit ergibt sich dann auch der Aufbau der folgenden Ausführungen: In einem ersten Schritt (B.) ist die den Verfassern bekannte bzw. öffentlich zugängliche Ausgestaltung des KiSS – unter Einschluss des Kreises der Zugriffsberechtigten – zu skizzieren, um sodann nach den einschlägigen datenschutzrechtlichen Vorgaben mit besonderem Akzent auf der Problematik des Kreises der Zugriffsberechtigten zu fragen und diese in Bezug auf das KiSS bzw. auch andere, ähnlich strukturierte Informationssysteme zu konkretisieren (C.). Die Studie schliesst mit einer Zusammenfassung der Ergebnisse in Thesenform sowie einigen abschliessenden Bemerkungen (D.).

Die vorliegende Untersuchung geht auf ein durch die Verfasser erstelltes Gutachten zurück. Inhaltlich handelte es sich um ein unabhängiges Gutachten: Die Verfasser wurden ausdrücklich nicht auf eine vorgefasste Ansicht oder ein

---

359, E. 6.4; BGE 126 II 126, E. 5; relativierend auch *Gächter/Egli*, Jusletter v. 6.9.2010, Rn. 279 f.; wie hier wohl auch *Meier*, Protection des données, Rn. 631. Ausführlich zur Tragweite des Art. 8 EMRK *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 9 ff.; zur Tragweite des Art. 13 BV im Einzelnen *Belser*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 6, Rn. 56 ff.

[3] Zur Abgrenzung des Anwendungsbereichs des DSG und der kantonalen Datenschutzgesetze noch unten C.I.

vorgegebenes Ergebnis verpflichtet, sondern um eine unabhängige Klärung der sich stellenden Fragen gebeten.

B. Das Klienten-Informationssystem für Sozialarbeit (KiSS) – eine Skizze

Beim **Klienten-Informationssystem für Sozialarbeit (KiSS)** handelt es sich um eine **Informationssystem-Software**, die im Sozialwesen tätige Behörden (oder private Organisationen) bei der **Verwaltung ihrer „Klienten"-Informationen** unterstützt, indem dieselben in sachdienlicher Art und Weise zur Verfügung gestellt und aufbereitet werden.

Die Software stellt verschiedene, miteinander **kombinierbare Module** zur Verfügung, in denen bestimmte (auch besonders schützenswerte) Personendaten gespeichert werden können. Zudem ermöglicht es das System, „per Mausklick" das soziale Umfeld der Klienten optisch zusammenzufassen.[4] Im Zusammenhang mit der vorliegenden Untersuchung sind folgende Module, die von gewissen Behörden in auf deren Bedürfnisse zugeschnittenen Ausführungen genutzt werden, von Bedeutung:

- Das **Basis-Modul** (B-Modul) enthält die Personalien der jeweiligen Klienten und Angaben der Einwohnerkontrolle. Es handelt sich um ein rein administratives Modul, welches allerdings einen Hinweis auf andere Module enthält, in welchen ebenfalls Informationen über die Person gespeichert sind, deren Angaben im B-Modul enthalten sind.
- Das **Fallführungs-Modul** (F-Modul) stellt den zentralen Bestandteil der Software dar. In diesem Modul werden alle über die Klienten verfügbaren Akten (Besprechungsdokumentation, Korrespondenzen, Bemerkungen der Sozialarbeiter über die Klienten usw.) elektronisch abgelegt.[5] Ferner enthält das Modul eine Grafik, welche die Struktur der Familie (inkl. Namen, Verwandtschaftsgrad usw.) visualisiert (sog. „Sozialsystem"). Auch aus diesem Modul ist ersichtlich, bei welchen anderen Modulen je-

---

[4] Vgl. Prospekt BEDAG, abrufbar im Internet unter <http://www.bedag.ch/fileadmin/Media/Dienstleistungen/Software-Entwicklung/Fachloesungen/01-14_KiSS_d.pdf> (zuletzt besucht am 17.1.2014): „Zum Beispiel, wenn parallel zur Sozialhilfe ein Inkassoverfahren läuft und eine Beistandschaft errichtet wird."

[5] Es handelt sich hierbei zu einem grossen Teil um besonders schützenswerte Personendaten im Sinne der Datenschutzgesetzgebung. Vgl. die Definition der besonders schützenswerten in Art. 3 KDSG, der in lit. c. auch Angaben über „Massnahmen der sozialen Hilfe oder fürsorgerischer Betreuung" nennt.

weils weitere Informationen über die betroffene Person gespeichert sind.
- Das **Sozialhilfe-Modul** (S-Modul), das **Vormundschafts-Modul** (V-Modul) und das **Inkassomodul** (I-Modul) enthalten jeweils die entsprechenden themenspezifischen Informationen.

In aller Regel werden diese Module bzw. einige derselben von zwei oder mehreren Ämtern einer kantonalen oder insbesondere auch kommunalen Verwaltung genutzt werden, so z.B. vom für die Sozialhilfe zuständigen Amt bzw. Dienst oder dem für Kindes- und Erwachsenenschutz zuständigen Amt. Diese Behörden sind für die Erfüllung ihrer **gesetzlichen Aufgaben** regelmässig darauf angewiesen, Personendaten zu bearbeiten. So muss etwa im Rahmen der Prüfung von Ansprüchen aus der Sozialhilfe das für die Gewährung derselben zuständige Amt verschiedene persönliche Voraussetzungen der Antragssteller prüfen, um im Anschluss auf der Grundlage dieser Informationen – welche Personendaten im Sinne der Datenschutzgesetzgebung darstellen,[6] die auf verschiedene Art und Weise (Beschaffung, Übernahme in das Dossier, u.a.m.) bearbeitet werden – über allfällige Leistungen entscheiden zu können. Die Verwaltung der Dossiers geschieht hierbei mittels eines softwaregestützten Informationssystems, welches auf die jeweiligen Behörden und ihre Aufgaben individuell zugeschnitten ist.

Im Einzelnen ergeben sich die hier massgeblichen gesetzlichen Aufgaben aus der einschlägigen (kantonalen) Spezialgesetzgebung, aus der sich häufig auch die Grundzüge der Wahrnehmung dieser Aufgaben sowie der Organisation ergeben, die dann häufig auf dem Verordnungsweg konkretisiert werden. Auf dieser Grundlage erschliessen sich dann auch die konkret von den verschiedenen Sektionen oder Abteilungen eines Amts wahrgenommenen Aufgaben, was wiederum für die Frage relevant ist, zu welchen Daten die in den jeweiligen Sektionen tätigen Personen Zugriff haben müssen bzw. dürfen.

---

[6] Vgl. die Definition in Art. 2 Abs. 1 KDSG, wonach Personendaten Angaben über eine bestimmte oder bestimmbare natürliche (oder juristische) Person sind. Zum Begriff der Personendaten ausführlich *Belser/Noureddine*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 7, Rn. 36 ff.; *Meier*, Protection des données, § 3, Rn. 418 ff.

C. Datenschutzrechtliche Vorgaben für Errichtung und Betrieb von Informationssystemen – am Beispiel des Klienten-Informationssystems für Sozialarbeit (KiSS) und unter besonderer Berücksichtigung des Kreises der Zugriffsberechtigten

Im Zentrum des folgenden Abschnitts sollen die bei der Errichtung und dem Betrieb von Informationssystemen wie dem KiSS zur Anwendung kommenden rechtlichen Vorgaben aufgezeigt werden, wobei der Akzent auf dem Kreis der jeweils zugriffsberechtigten Personen bzw. Stellen liegt und – wie bereits eingangs erwähnt[7] – beispielhaft auf das Recht des Kantons Bern Bezug genommen wird. Im Einzelnen kann auf der Grundlage der Klarstellung des anwendbaren Rechts (I.) zwischen dem Grundsatz der Rechtmässigkeit und dem Erfordernis einer gesetzlichen Grundlage (II.), der Beachtung der Grundsätze der Zweckbindung (III.) und der Verhältnismässigkeit (IV.) sowie weiteren Anforderungen (V.) unterschieden werden.

I. Zum anwendbaren Recht

Der Anwendungsbereich des Schweizerischen Datenschutzgesetzes (DSG) erstreckt sich auf die Bearbeitung von Personendaten von natürlichen und juristischen Personen durch private Personen und Bundesorgane (Art. 2 Abs. 1 DSG).[8] Aufgrund der Kompetenzverteilung der Bundesverfassung ist die Regelung der **Bearbeitung von Personendaten** durch **kantonale und kommunale Behörden** Sache der **Kantone**.

Die Datenbearbeitung durch **kantonale Behörden** fällt selbst dann nicht unter das DSG, wenn diese mit dem Vollzug von Bundesrecht betraut sind (Art. 2 Abs. 1 lit. b DSG, s. auch Art. 37 DSG). Dies erklärt sich durch die in der Bundesverfassung vorgesehene Kompetenzverteilung zwischen Bund und Kantonen, wonach eine Kompetenz des Bundes nur dann vorliegt, wenn diese ausdrücklich in der Verfassung vorgesehen ist. So kennt die Verfassung keine Bestimmung, die die Aufgabe des Datenschutzes explizit dem Bund zuweist und ihn zu einer umfassenden Regelung des Datenschutzes ermächtigt; gleichwohl kommen dem

---

[7] Oben A.

[8] Das Gesetz wurde gestützt auf Art. 95, 122 und 173 Abs. 2 BV erlassen.

Bundesgesetzgeber auch in diesem Bereich gewisse Kompetenzen zu, denn er kann immer dann (auch) datenschutzrechtliche Fragen im Rahmen einer Annexkompetenz „mitregeln", wenn ihm für den betreffenden Bereich eine entsprechende Sachkompetenz zukommt. Insofern stützt sich der Bundesgesetzgeber zum Erlass von Datenschutzrecht auf Annexkompetenzen zu seinen Sachkompetenzen, wobei Art. 122 Abs. 1 BV (Zivilrecht), Art. 123 Abs. 1 BV (Strafrecht) sowie die entsprechenden Kompetenzen zum Erlass von Prozessrecht und Art. 164 Abs. 1 lit. g BV als Kompetenz, Organisation und Verfahren der Bundesbehörden zu regeln, von besonderer Bedeutung sind.

Damit kommen für die Datenbearbeitung im Umfeld der Sozialhilfe – die in dieser Studie beispielhaft für das Aufzeigen der datenschutzrechtlichen Anforderungen für die Errichtung und den Betrieb von Informationssystemen herausgegriffen wird[9] – in aller Regel die **kantonalen Datenschutzgesetze** zur Anwendung, geht es hier doch um in der Zuständigkeit der Kantone liegende Fragen. Abgrenzungsfragen – die insbesondere dann relevant werden können, wenn die Wahrnehmung öffentlicher Aufgaben auf (öffentliche oder private) Institutionen übertragen wird – stellen sich im Zusammenhang mit der hier im Vordergrund stehenden Fragestellung nicht.[10]

Wie bereits erwähnt,[11] soll dabei beispielhaft auf die **Datenschutzgesetzgebung des Kantons Bern** Bezug genommen werden. Her sind das **Datenschutzgesetz (KDSG)**[12] und die **Datenschutzverordnung (DSV)**[13] des Kantons Bern von besonderer Bedeutung. Hinzuweisen ist aber auch auf möglicherweise einschlägige **spezialgesetzliche Bestimmungen** (etwa das KESG oder das SHG) sowie die zugehörigen Verordnungen, dies insbesondere im Zusammenhang mit der Frage nach der Existenz einer Rechtsgrundlage für die Datenbearbeitung.

Die Verfassung des Kantons Bern[14] – insbesondere der Datenschutzartikel (Art. 18 Abs. 2 KV-BE) – kann vernachlässigt werden, weil ihre Ansprüche nicht über diejenigen der BV hinausgehen bzw. mit ihnen übereinstimmen.[15]

---

9 Oben A.

10 Vgl. zu diesen, m.w.N., *Epiney*, in: Verwaltungsorganisationsrecht, 5 (11 ff.).

11 Oben A.

12 Datenschutzgesetz vom 19. Februar 1986 (KDSG), BSG 152.04.

13 Datenschutzverordnung vom 22. Oktober 2008 (DSV), BSG 152.040.1.

14 Verfassung des Kantons Bern vom 6. Juni 1993, BSG 101.1.

15 Betreffend Art. 18 Abs. 2 KV-BE offen gelassen – allerdings mit dem Hinweis, dass der Verfassungsartikel keine subjektiven Rechte vermittle, sondern sich an den Gesetzgeber richte – in BGer, 8C_949/2011, Urt. v. 4.9.2012, E. 5.1.

Da die kantonalen Datenschutzgesetze – so auch das Gesetz des Kantons Bern – jedoch in weiten Teilen Grundsätze enthalten, die auch auf Bundesebene im DSG geregelt sind und die (allgemeinen) datenschutzrechtlichen Grundsätze (wie insbesondere die hier im Vordergrund stehenden Grundsätze der Rechtmässigkeit, der Zweckbindung und der Verhältnismässigkeit) im Übrigen letztlich Konkretisierungen des Art. 13 BV sowie des Art. 8 EMRK darstellen, kann bei der Auslegung des kantonalen Rechts auch auf die **entsprechenden Grundsätze des DSG** und ihre Auslegung in Literatur und Rechtsprechung zurückgegriffen werden, ganz abgesehen davon, dass die Vorgaben der **Verfassung** und der **EMRK**[16] sowieso bei der Auslegung des kantonalen Rechts zu beachten sind.

Im Übrigen – wohl auch und gerade vor dem Hintergrund der erwähnten verfassungs- und europarechtlichen Vorgaben – sind die **kantonalen Datenschutzgesetze weitgehend parallel** ausgestaltet,[17] so dass die Ergebnisse der vorliegenden Untersuchung grundsätzlich auch auf die Rechtslage in anderen Kantonen übertragen werden können.

Die Bearbeitung von Personendaten durch öffentliche Organe stellt grundsätzlich einen Eingriff in die durch die Verfassung gewährten Persönlichkeitsrechte der Betroffenen dar. Konkret handelt es sich um einen Eingriff in den Schutzbereich sowohl von Art. 8 EMRK[18] als auch von Art. 13 Abs. 2 BV.[19] Eine Rechtfertigung ist möglich, wenn die Voraussetzungen von Art. 8 Abs. 2 EMRK bzw. Art. 36 BV gegeben sind.[20] Zwingende Voraussetzung ist somit

---

16 Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) vom 4.11.1950 (SR 0.101).

17 Vgl. zum kantonalen Datenschutzrecht im Einzelnen *Waldmann/Oeschger*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, die auch und gerade die weitgehende Parallelität der kantonalen Gesetzgebung herausarbeiten.

18 *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 9 ff., m.w.N. Vgl. die sog. „Leander-Rechtsprechung" des EGMR, EGMR, Urt. v. 26.3.1987, Serie A, Bd. 116 (Leander/Schweden); s. auch EGMR, Urt. v. 18.10.2011, Nr. 16188/07 (Khelili/Schweiz); BGer, 8C_949/2011, Urt. v. 4.9.012, E. 5.2, m.w.N.: „Bei der Frage, ob ein Eingriff im Sinn von Art. 8 Ziff. 2 EMRK vorliegt, berücksichtigt der EGMR die Art der Information, die Form ihrer Verwendung und das Ergebnis, zu dem diese führen kann […]."

19 *Belser*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 6, Rn. 115 ff. (allerdings teilweise kritisch vor dem Hintergrund der Infragestellung des Konzepts der „informationellen Selbstbestimmung"); aus der Rechtsprechung BGE 128 II 259, E. 3.2; BGE 129 I 232, E. 4.3.1.; BGE 138 II 346, E. 8.2 (Datenbearbeitung durch Private), m.w.N.

20 *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 17 ff.; *Belser*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 6, Rn. 122 ff., jeweils m.w.N.

eine gesetzliche Grundlage für, ein öffentliches Interesse an (das in der gesetzlichen Grundlage zu benennen ist) und die Verhältnismässigkeit der Bearbeitung von Personendaten. Diese Grundsätze werden – wie erwähnt – in der Datenschutzgesetzgebung konkretisiert.

II. Zum Grundsatz der Rechtmässigkeit und dem Erfordernis einer gesetzlichen Grundlage

1. Grundsätze

a) Gesetzliche Grundlage

Personendaten dürfen nur rechtmässig bearbeitet[21] werden (**Grundsatz der Rechtmässigkeit**), was etwa in Art. 4 Abs. 1 DSG ausdrücklich verankert ist. Für öffentliche Organe wurde dieser Grundsatz in dem Sinn konkretisiert, dass eine Datenbearbeitung grundsätzlich eine **gesetzliche Grundlage** voraussetzt, wie dies auch in Art. 5 Abs. 1 KDSG vorgesehen ist. Danach dürfen Personendaten nur bearbeitet werden, „wenn das Gesetz ausdrücklich dazu ermächtigt oder wenn das Bearbeiten der Erfüllung einer gesetzlichen Aufgabe dient". Erforderlich ist eine gesetzliche Grundlage somit immer, entweder als Grundlage für die Bearbeitung von Personendaten oder als Grundlage für eine staatliche Aufgabe, deren Erfüllung die Bearbeitung von Personendaten erfordert.

b) Erhöhte Anforderungen in Bezug auf besonders schützenswerte Personendaten

Erhöhten Anforderungen muss die gesetzliche Grundlage genügen, wenn **besonders schützenswerte Personendaten** bearbeitet werden.

Nach der Legaldefinition in Art. 3 KDSG sind hierunter Angaben über die religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung, die Rasse, Massnahmen der sozialen Hilfe oder der fürsorgerischen Betreuung, den persönlichen Geheimbereich (insbesondere die Gesundheit), sowie über polizeiliche Ermittlungen, Strafverfahren, Straftaten oder verhängte Strafen bzw. Massnahmen zu verstehen.

---

[21] Die Bearbeitung umfasst jeglichen Umgang mit Personendaten, vgl. Art. 2 Abs. 4 KDSG, so dass z.B. auch allein die Einsicht von Mitarbeitenden einer Behörde in bestimmte Daten erfasst wird, liegt hier doch aus datenschutzrechtlicher Sicht eine Bekanntgabe vor.

Diese erhöhten Anforderungen an die Rechtmässigkeit der Bearbeitung besonders schützenswerter Personendaten und damit die rechtliche Grundlage (bzw. die zulässigen Ausnahmen von derselben) ergeben sich im Ansatz bereits aus **Art. 8 EMRK**: So geht der Gerichtshof für Menschenrechte in ständiger Rechtsprechung davon aus, dass für bestimmte Kategorien von Eingriffen in Art. 8 EMRK unterschiedlich weitgehende Vorgaben an die Qualität der gesetzlichen Grundlage zum Zuge kommen, so dass für besondere Gruppen von (angesichts der Reichweite der möglichen Persönlichkeitsbeeinträchtigung bzw. der Beeinträchtigung der Privatsphäre) eher schweren Eingriffen erhöhte Anforderungen gestellt werden.[22]

Im Übrigen ergibt sich auch bereits aus dem **Gesetzmässigkeitsprinzip**, dass die Anforderungen an die Präzision und Form der gesetzlichen Grundlage mit der Intensität der Datenbearbeitungen bzw. mit dem Risikopotenzial für allfällige Persönlichkeitsverletzungen steigen. Sobald also in einem gewissen Umfang und mit einer gewissen „Verbreitung" (was die Zugangsberechtigten angeht) besonders schützenswerte Daten bearbeitet werden, ist die gesetzliche Grundlage sehr genau zu fassen, und grundsätzlich ist eine formell-gesetzliche Grundlage notwendig. In diesem Sinn formuliert auch Art. 36 Abs. 1 S. 2, dass schwerwiegende Einschränkungen von Grundrechten im Gesetz selbst (also in einer formell-gesetzlichen Grundlage) vorgesehen sein müssen, eine Vorgabe, die auch für die kantonale Ebene von Bedeutung ist.[23] Dies schliesst Surrogate einer solchen ausdrücklichen gesetzlichen Grundlage nicht von vornherein aus, setzt ihrer Ausgestaltung jedoch gewisse (wohl eher enge) Grenzen.

Vor diesem Hintergrund erschliesst sich auch die Bedeutung des Art. 6 KDSG,[24] wonach besonders schützenswerte Personendaten lediglich bearbeitet werden dürfen, wenn zusätzlich zu den allgemeinen Anforderungen nach Art. 5 KDSG die „Zulässigkeit sich

---

[22] Vgl. zur Rechtsprechung des EGMR zu dieser Problematik, m.w.N., *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, Rn. 17.

[23] Vgl. zur Rechtsprechung des EGMR zu dieser Problematik, m.w.N., *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, Rn. 17; zu den verfassungsrechtlichen Vorgaben *Belser*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 6, Rn. 6 ff.; s. auch *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 51.

[24] Vgl. für die Regelung in anderen Kantonen, die sich (ebenfalls) weitgehend an die bundesrechtliche Regelung anlehnen, die Nachweise bei *Waldmann/Oeschger*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, Rn. 42.

aus einer gesetzlichen Grundlage klar ergibt, oder (…) die Erfüllung einer gesetzlichen Aufgabe es zwingend erfordert, oder (…) die betroffene Person ausdrücklich zugestimmt hat". Angesichts des Umstands, dass bereits Art. 5 Abs. 1 KDSG entweder eine gesetzliche Grundlage oder die Erfüllung einer gesetzlichen Aufgabe voraussetzt und der erwähnten verfassungs- und europarechtlichen Vorgaben, ist zu folgern, dass die Anforderungen in Art. 6 KDSG offenbar strenger auszulegen sind, was sich aus dem Wortlaut der Bestimmung bei der ersten Alternative nicht klar ergibt.[25] Vor diesem Hintergrund können die **Anforderungen des Art. 6 KDSG** wie folgt (zumindest etwas[26]) präzisiert werden.

Hinzuweisen ist in diesem Zusammenhang auch auf die entsprechende bundesrechtliche Regelung: So dürfen besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nach Art. 17 Abs. 2 DSG grundsätzlich nur bearbeitet werden, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht. „Ausnahmsweise" ist eine Bearbeitung solcher Daten nach dieser Bestimmung auch zulässig, wenn (u.a.) diese für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe „unentbehrlich" ist oder die betroffene Person im Einzelfall eingewilligt hat. Die kantonalen Datenschutzgesetze enthalten in der Regel ähnliche Bestimmungen.[27]

aa) Klare gesetzliche Grundlage (Art. 6 lit. a KDSG)

Eine **gesetzliche Grundlage** muss die Datenbearbeitung **klar** auch auf **besonders schützenswerte Personendaten** beziehen. Im Übrigen muss die gesetzliche Grundlage **hinreichend bestimmt** sein, wozu insbesondere die klare Umschreibung des Bearbeitungszwecks (vgl. auch schon Art. 5 Abs. 2 KDSG), der Art und des Umfangs der Datenbearbeitung, der an der Datenbearbeitung Beteiligten sowie der Kategorien der bearbeiteten Daten gehören dürften.[28]

---

[25] So ist eine „klare" (vgl. Art. 6 KDSG) nicht zwingend „strenger" als eine „ausdrückliche" (vgl. Art. 5 Abs. 1 KDSG) Regelung.

[26] Insbesondere bei Art. 6 lit. a, b KDSG kommt es auch auf den Einzelfall an, hängen doch die Anforderungen etwa an die Bestimmtheit der gesetzlichen Grundlage von der Intensität der (möglichen) Persönlichkeitsverletzung ab, vgl. zum Ganzen (in Bezug auf die Bundesebene) *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 41 ff.

[27] Vgl. die Nachweise bei *Waldmann/Oeschger*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, Rn. 42.

[28] Vgl. insoweit schon, m.w.N., *Epiney/Civitella/Zbinden*, Datenschutzrecht, 40; *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 44 ff.

Im Übrigen ergibt sich – wie erwähnt[29] – aus dem Gesetzmässigkeitsprinzip, dass die Anforderungen an die Präzision der gesetzlichen Grundlage mit der Intensität der Datenbearbeitungen bzw. mit dem Risikopotenzial für allfällige Persönlichkeitsverletzungen steigen. Sobald also in einem gewissen Umfang und mit einer gewissen „Verbreitung" (was die Zugangsberechtigten angeht) besonders schützenswerte Daten bearbeitet werden, ist die gesetzliche Grundlage sehr genau zu fassen.

Dabei spricht Vieles dafür, dass – auch wenn dies in Art. 6 KDSG nicht präzisiert wird – grundsätzlich nur eine **formell-gesetzliche Grundlage** ausreichend ist, sind doch nach den allgemeinen Grundsätzen des Gesetzmässigkeitsprinzips die wesentlichen Entscheidungen in einem Gesetz im formellen Sinn zu verankern. Bei Bearbeitungen von besonders schützenswerten Personendaten in einem gewissen Umfang dürfte regelmässig vom Vorliegen dieser Voraussetzung auszugehen sein, wobei es in diesem Zusammenhang auch bezeichnend ist, dass auf Bundesebene Art. 17 Abs. 2 DSG ausdrücklich auf ein Gesetz im formellen Sinn verweist.

bb) Zwingende Notwendigkeit zur Erfüllung einer gesetzlichen Aufgabe (Art. 6 lit. b KDSG)

Auch wenn keine eigentliche gesetzliche Grundlage vorhanden ist, ist eine Bearbeitung besonders schützenswerter Personendaten weiter dann zulässig, wenn sie zur **Erfüllung einer gesetzlichen Aufgabe „zwingend" erforderlich** ist, ein Surrogat für eine Rechtsgrundlage, das sich – in teilweise leicht abweichender Formulierung – auch auf Bundesebene (vgl. Art. 17 Abs. 2 lit. a DSG, der den Begriff „unentbehrlich" verwendet) und in den anderen kantonalen Datenschutzgesetzen[30] findet.

Offensichtlich ist es also nicht ausreichend, dass die Datenbearbeitung im Hinblick auf die Erfüllung der gesetzlichen Aufgabe hilfreich ist oder dieser (nur) dient (wie dies in Art. 5 Abs. 1 KDSG formuliert ist), sondern die Erfüllung der gesetzlichen Aufgabe darf ohne die Bearbeitung der besonders schützenswerten Personendaten nicht möglich sein. M.a.W. würde die Erfüllung der Aufgabe ohne die fragliche Datenbearbeitung geradezu **vereitelt**,[31] so dass es

---

[29] Oben C.III.1.b), am Anfang.

[30] Vgl. die Nachweise für die Formulierungen in den kantonalen Datenschutzgesetzen bei *Waldmann/Oeschger*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, Rn. 42.

[31] Vgl. mit Bezug auf die entsprechende Vorschrift im DSG (Art. 17 Abs. 2 lit. a DSG) *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 17, Rn. 77;

nicht ausreichend ist, dass die Datenbearbeitung die Wahrnehmung der gesetzlichen Aufgabe erleichterte oder effizienter gestaltete.

Diese Anforderung dürfte sich nicht nur auf den **Grundsatz der Bearbeitung besonders schützenswerter Personendaten**, sondern auch auf die genaue **Ausgestaltung** derselben (Umfang der Datenbearbeitung, Ausgestaltung des Zugangs u.a.m.) beziehen. Denn nur dieser Ansatz trägt wohl dem systematischen Zusammenhang mit Art. 5 Abs. 3 KDSG, der den Grundsatz der Verhältnismässigkeit verankert, Rechnung: Nach dem Wortlaut des Art. 6 KDSG und dem Zusammenhang mit Art. 5 KDSG geht es in Art. 6 KDSG um zusätzliche, also weitergehende Anforderungen an die Zulässigkeit der Datenbearbeitung. Bezöge man nun die Anforderung des Art. 6 lit. b KDSG nur auf den Grundsatz der Bearbeitung besonders schützenswerter Personendaten, nicht aber auch ihre konkrete Ausgestaltung, so wären im Ergebnis kaum zusätzliche Anforderungen zu beachten (wird doch der Grundsatz der Bearbeitung bestimmter besonders schützenswerter Personendaten in zahlreichen Fällen zur Erfüllung einer gesetzlichen Aufgabe zwingend notwendig sein), sondern es ginge letztlich (nur) um die Einhaltung des Verhältnismässigkeitsgrundsatzes, der sowieso bei jeder Datenbearbeitung zu beachten ist. Im Übrigen und vor allem widerspräche es Sinn und Zweck des Art. 6 lit. b KDSG, die zwingende Erforderlichkeit nur auf den Grundsatz, nicht aber die Modalitäten der Datenbearbeitung zu beziehen: Denn die Vorschrift will offenbar sicherstellen, dass in dieser Konstellation besonders schützenswerte Personendaten nur unter der Voraussetzung bearbeitet werden, dass dies zwingend zur Wahrnehmung einer gesetzlichen Aufgabe notwendig ist, dies im Hinblick auf den verfassungsrechtlich gebotenen Schutz der Persönlichkeit. Unterschiede man nun zwischen Grundsatz und Modalitäten, würde diese Zielsetzung unterlaufen, implizierte ein derartiger Ansatz doch, dass gewisse Bearbeitungen erfolgten, die gerade nicht zwingend für die Wahrnehmung der gesetzlichen Aufgabe notwendig sind (z.B. eine Aufbewahrung besonders schützenswerter Personendaten, ohne dass dies für die Erfüllung der gesetzlichen Aufgabe zwingend erforderlich wäre, sondern dieser nur dient, ihre Wahrnehmung also erleichtert wird).

Botschaft DSG, BBl 1988 II 468; *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 53; in Bezug auf entsprechende kantonale Regelungen *Waldmann/Oeschger*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, Rn. 42.

Deutlich wird damit auch, dass sich die aus Art. 6 lit. b KDSG ergebenden Anforderungen teilweise mit den allgemeinen Grundsätzen der Zweckbindung und der Verhältnismässigkeit überschneiden, ist es doch z.B. auch eine Frage der Verhältnismässigkeit, ob die Bearbeitung einer bestimmten Angabe zur Erfüllung der gesetzlichen Aufgabe (zwingend) erforderlich ist. Im Übrigen dürfte eine Datenbearbeitung von vornherein nur dann zur Erfüllung einer gesetzlichen Aufgabe zwingend erforderlich sein, wenn sie den Anforderungen der Geeignetheit und der Erforderlichkeit (also des mildesten Mittels in Bezug auf die Beeinträchtigung der Persönlichkeitsrechte der Betroffenen) entspricht. Gute Gründe, insbesondere der bereits erwähnte Zusammenhang mit Art. 5 KDSG, der mit der Vorschrift angestrebte Zweck eines effektiven und weitergehenden Schutzes besonders schützenswerter Personendaten sowie der verfassungs- und menschenrechtlich gebotene Schutz dieser Daten, sprechen hier dafür, dass die **Anforderungen an den „zwingenden" Charakter der Datenbearbeitung** zur Erfüllung des gesetzlichen Zwecks tendenziell **strenger** sind als diejenigen der **„normalen" Erforderlichkeit im Rahmen der Verhältnismässigkeitsprüfung**. Dieser Grundsatz wird insbesondere in der bereits erwähnten Anforderung konkretisiert, dass die Datenbearbeitung (inklusive ihrer Modalitäten) für die Erfüllung der gesetzlichen Aufgabe nicht nur nützlich oder hilfreich, sondern zwingend erforderlich sein muss, so dass allein eine erhöhte Effizienz o.ä. gerade nicht ausreichend ist.

Auch ist es für die Frage, ob die Voraussetzungen des Art. 6 lit. b KDSG vorliegen, unerheblich, ob die mit den fraglichen Datenbearbeitungen befassten Personen einer (gesetzlich vorgesehenen) Schweigepflicht oder einem Amtsgeheimnis unterliegen. Denn diese Aspekte stehen mit den Anforderungen des Rechtmässigkeitsprinzips nicht im Zusammenhang; dieses ist vielmehr unabhängig von derartigen Pflichten zu beachten. Insbesondere kann aus diesen Pflichten nicht abgeleitet werden, dass einer solchen Schweigepflicht unterstehende Personen eine Art erleichterter Zugang zu Daten haben dürften.[32]

Weiter wird man verlangen müssen, dass die **gesetzliche Aufgabe hinreichend bestimmt** umschrieben ist, kann doch nur auf dieser Grundlage eruiert werden, ob die entsprechende Datenbearbeitung für ihre Erfüllung unentbehrlich ist.[33] Schliesslich spricht auch hier das Gesetzmässigkeitsprinzip dafür, dass grundsätzlich ein Gesetz im formellen Sinn notwendig ist (wie dies auch auf Bundesebene in Art. 17 Abs. 2 lit. a DSG verankert ist).

Fraglich könnte in diesem Zusammenhang noch sein, ob eine solche Datenbearbeitung nur im **Einzelfall** erfolgen darf, womit eine systematische und re-

---

[32] Zumindest missverständlich jedoch BGE 133 V 359. Vgl. zu dieser Problematik im Zusammenhang mit Krankenversicherungsdaten *Uttinger*, HAVE 2007, 253 ff.

[33] In diese Richtung auch wohl die bundesgerichtliche Rechtsprechung in Bezug auf Art. 17 Abs. 2 lit. a DSG, vgl. BGE 124 III 170 E. 4a. Ausdrücklich auch z.B. *Jöhri/Studer*, in: Mauer-Lambrou/Vogt, BK Datenschutzgesetz, Art. 17, Rn. 47.

gelmässige Datenbearbeitung nicht im Einklang stünde. Dieser Ansatz wird im Zusammenhang mit Art. 17 Abs. 2 DSG mit dem Argument vertreten, diese Bestimmung sehe die in Art. 17 Abs. 2 lit. a-c DSG genannten Konstellationen ausdrücklich als „Ausnahmekonstellationen" vor.[34] Dieses Argument greift jedoch bei Art. 6 KDSG nicht, da hier die drei Buchstaben „gleichberechtigt" nebeneinander stehen. Immerhin sei aber darauf hingewiesen, dass sich aus den allgemeinen Grundsätzen des Gesetzmässigkeitsprinzips ergeben dürfte, dass bei Bearbeitungen besonders schützenswerter Personendaten in einem gewissen Umfang und einer gewissen Regelmässigkeit eine gesetzliche Grundlage notwendig erscheint, geht es hier doch um wichtige rechtsetzende Bestimmungen sowie um Massnahmen, mit denen ein gewisses Risiko für Persönlichkeitsverletzungen verbunden ist.[35]

cc) Ausdrückliche Zustimmung (Art. 6 lit. c KDSG)

Von einer **ausdrücklichen Zustimmung** – welche im Übrigen auch für „normale" Personendaten zulässig wäre (*a maiore ad minus*)[36] – kann nur dann ausgegangen werden, wenn sowohl ihr Inhalt (also der Bezug zu einer bestimmten, ggf. näher präzisierten Datenbearbeitung, so dass die Zustimmung klar sein muss und eine umfassende Information über Art und Umfang der Datenbearbeitung voraussetzt) als auch die Form ausdrücklich erfolgt bzw. ist, so dass jedenfalls eine klare und zweifelsfreie Einverständniserklärung zu fordern ist, die zumindest in der Regel nicht konkludent erfolgen kann.[37] Jedenfalls fallen die Anforderungen an die Einwilligung umso höher aus, je stärker der Eingriff in die Persönlichkeitsrechte der betroffenen Person ist.[38]

---

[34] *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 17, Rn. 76; *Jöhri/Studer*, in: Mauer-Lambrou/Vogt, BK Datenschutzgesetz, Art. 17, Rn. 47; so auch EDÖB, Empfehlung betreffend Drogen- und Alkoholtestes bei den SBB v. 25.5.2007, Ziff. II.6.

[35] Vgl. auch noch unten C.II.2.a), am Ende, sowie D.II.

[36] Vgl. (in Bezug auf Art. 17 Abs. 2 lit. c DSG) etwa *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 52.

[37] Vgl. im Einzelnen *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 19, m.w.N. zur Frage, ob auch eine konkludente Einwilligung „ausdrücklich" sein kann.

[38] *Wermelinger/Schweri*, Jusletter v. 3.3.2008, Rn. 13; *Schweizer*, Data Mining, 180 ff.; a.A. aber *Weber*, Datenschutzrecht vor neuen Herausforderungen, 34.

2. *Anwendung auf das Klienten-Informationssystem für Sozialarbeit (KiSS)*

Im Folgenden sollen die erörterten, sich aus dem Grundsatz der Rechtmässigkeit ergebenden allgemeinen Anforderungen an die Errichtung und den Betrieb von Informationssystemen, innerhalb derselben Personendaten bearbeitet werden, für den Rückgriff auf das Klienten-Informationssystem für Sozialarbeit (KiSS) spezifiziert bzw. angewandt werden, wobei neben den Grundsätzen (a) der Frage nach der Reichweite der Zugriffsberechtigung (b) besondere Aufmerksamkeit geschenkt werden soll.

a) Grundsatz

Im Zusammenhang mit dem Klienten-Informationssystem für Sozialarbeit (KiSS) ist zunächst davon auszugehen, dass es grundsätzlich um die **Bearbeitung besonders schützenswerter Personendaten** geht: Denn die Legaldefinition des Art. 3 KDSG erwähnt hier neben Personendaten über die Gesundheit (Art. 3 lit. b KDSG) sowohl Angaben über Massnahmen der sozialen Hilfe als auch über die fürsorgerische Betreuung (Art. 3 lit. c KDSG).[39] Zwar sind im B-Modul (Basis-Modul) lediglich die Personalien der jeweiligen Klienten und Angaben der Einwohnerkontrolle gespeichert,[40] wobei es sich nicht um besonders schützenswerte Personendaten handelt. Jedoch stellt dieses Modul ein rein administratives Modul dar, und der Zugang zum B-Modul ist immer mit dem Zugang zu mindestens einem anderen Modul gekoppelt.[41] In diesen anderen Modulen figurieren aber Daten über Sozialhilfe sowie die fürsorgerische Betreuung, möglicherweise auch weitere besonders schützenswerte Daten (etwa solche über die Gesundheit oder andere Angaben, die in Korrespondenzen Eingang gefunden haben).[42] Insofern ist davon auszugehen, dass die im Rahmen des KiSS erfolgende Datenbearbeitung durchwegs[43] besonders schützenswerte Personendaten betrifft

---

[39] Vgl. zu Art. 3 lit. c DSG *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 3, Rn. 42 ff. Im Übrigen dürfte es sich bei den in den Modulen enthaltenen Personendaten regelmässig auch um Persönlichkeitsprofile i.S.v. Art. 3 lit. d DSG handeln.

[40] S.o. B.

[41] Vgl. oben B.

[42] Vgl. zum Inhalt der Module oben B.

[43] Allenfalls abgesehen vom Inkassomodul, das in der vorliegenden Untersuchung jedoch nicht im Vordergrund steht.

und damit die diesbezüglichen (strengeren) Anforderungen zu beachten sind.[44] Eine im Rahmen des KiSS erfolgende Datenbearbeitung muss somit den Vorgaben des Art. 6 KDSG entsprechen.

Die Bearbeitung von Personendaten – bspw. beim Zugriff auf das Informationssystem KiSS – stellt als solche einen Eingriff in die Persönlichkeitsrechte der Betroffenen dar, unabhängig davon, ob die jeweilige Mitarbeiterin oder der jeweilige Mitarbeiter der agierenden Behörde zu dieser Bearbeitung berechtigt ist.[45] Allerdings kann dieser Eingriff nach dem Gesagten gerechtfertigt und damit zulässig sein, dies allerdings nur, sofern er den dargelegten[46], sich letztlich bereits aus Art. 8 EMRK und Art. 13 Abs. 2 BV ergebenden Anforderungen entspricht.

Dabei ist davon auszugehen, dass eine **ausdrückliche Zustimmung** der betroffenen Person (vgl. Art. 6 lit. c KDSG) grundsätzlich **nicht gegeben** sein kann (was nicht ausschliesst, dass sie in einem Einzelfall vorliegen mag): Denn im Rahmen des KiSS werden die entsprechenden Informationen mehreren Personen bzw. Stellen zur Verfügung gestellt, die auf diese bis zu einem gewissen Grade kontextunabhängig zurückgreifen können, so dass es grundsätzlich nicht möglich erscheint, im Vorfeld „ausdrücklich" jedem Zugriff zuzustimmen, sind diese Zugriffe doch mitunter nicht vorhersehbar. Eine angemessene Information erscheint also bei solchen Informationssystemen in aller Regel schwierig bis unmöglich, so dass auch eine Zustimmung zu den entsprechenden Datenbearbeitungen nicht möglich ist. Auch ist zu bezweifeln, dass die Betroffenen tatsächlich umfassend über die Funktionsweise des KiSS informiert sind. Hinzu kommt, dass die Freiwilligkeit der Zustimmung im Kontext des KiSS zumindest in Frage gestellt werden kann, geht es doch grundsätzlich um Personen, die in einer irgendwie gearteten Notlage sind, so dass es zweifelhaft ist, ob ihre Ein-

---

[44] Im Übrigen dürfte es sich bei den in den Modulen enthaltenen Personendaten regelmässig auch um Persönlichkeitsprofile i.S.v. Art. 3 lit. d DSG handeln.

[45] Der Eingriff wiegt umso schwerer, wenn ein Mitarbeiter auf (besonders schützenswerte) Personendaten eines „Klienten" zugreift, welcher bspw. von einem anderen Mitarbeiter betreut wird. Vgl. (zu einem Informationssystem eines Spitals) Décision de la Commission cantonale de la protection des données du 23.2.2000 dans la procédure relative aux fichiers informatisés des données médicales des hôpitaux jurassiens, E 2.a: „Il résulte de ce qui précède que toute communication à un tiers, *même à un confrère médecin* [Hervorhebung durch die Verfasser], est en principe illicite, sauf s'il existe des motifs justificatifs."

[46] Oben C.II.1.

willigung in eine sie betreffende Datenbearbeitung wirklich aus freiem Willen erfolgt.[47]

Jedenfalls im Kanton Bern kann die Datenbearbeitung im Rahmen des KiSS auch nicht aufgrund ihrer „klaren" Verankerung in einer **gesetzlichen Grundlage** (im formellen oder materiellen Sinn)[48] zulässig sein (vgl. Art. 6 lit. a KDSG): Denn es ist kein Gesetz ersichtlich, dass die Datenbearbeitung im Rahmen des KiSS als solche in zumindest groben Zügen[49] vorsieht. Vielmehr wird das KiSS als solches in der einschlägigen Spezialgesetzgebung nicht erwähnt.

Allerdings könnte die Einrichtung und Betreibung des KiSS grundsätzlich deshalb mit dem Grundsatz der Rechtsmässigkeit vereinbar sein, weil es zur Erfüllung einer **gesetzlichen Aufgabe „zwingend" erforderlich** ist (Art. 6 lit. b KDSG). Ohne dass dieser Frage hier im Einzelnen nachgegangen werden kann, dürften im Ergebnis die besseren Gründe für eine **grundsätzliche Zulässigkeit des Rückgriffs auf das KiSS** unter diesem Gesichtspunkt sprechen. Denn in den hier in erster Linie möglicherweise einschlägigen Spezialgesetzen (KESG und SHG) werden den zuständigen Behörden bestimmte Aufgaben im Bereich des Kindes- und Erwachsenenschutzes einerseits und der Sozialhilfe andererseits zugewiesen:

- So sollen im Bereich der **Sozialhilfe** insbesondere Leistungsangebote der individuellen und der institutionellen Sozialhilfe bereitgestellt und Leistungen gewährt werden (Art. 4 Abs. 2 SHG). Dabei ist die Gewährung der Hilfe von gewissen Voraussetzungen (z.B. und insbesondere der Bedürftigkeit) abhängig (vgl. Art. 30 ff. SHG, wobei die Einzelheiten auf Verordnungsebene geregelt sind, s. zum Verfahren Art. 49 ff. SHG), und der Sozialdienst hat den relevanten Sachverhalt abzuklären.
- Das Amt für Erwachsenen- und Kindesschutz hat aufgrund von Art. 22 KESG (im Auftrag der zuständigen kantonalen Behörden) verschiedene Massnahmen im Bereich des **Kindes- und Erwachsenenschutzes** vorzunehmen.

Zur Wahrnehmung dieser gesetzlichen Aufgaben ist es für die zuständigen Behörden zwingend notwendig, über gewisse Angaben

---

[47] Vgl. zur Freiwilligkeit im Einzelnen *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 18.

[48] Wenn auch nach der hier vertretenen Ansicht grundsätzlich eine solche im formellen Sinn notwendig ist, s.o. C.II.1.b)aa).

[49] Vgl. zu den Anforderungen an die Bestimmtheit gesetzlicher Grundlagen bereits oben C.II.1.a), b)aa), bb).

in Bezug auf die betroffenen Personen zu verfügen, die auch und gerade besonders schützenswerte Personendaten umfassen. Denn nur auf diese Weise ist es möglich, das Vorliegen der jeweils relevanten gesetzlichen Voraussetzungen zu ermitteln bzw. die gesetzlich geforderten Massnahmen zu ergreifen. Ebenso dürfte die Aufbewahrung der Daten für eine gewisse Zeit und damit das Anlegen von Dossiers über die Betroffenen zur Erfüllung dieser Aufgaben notwendig sein. Damit ist auch die **Einrichtung eines Informationssystems nach Art. 6 lit. b KDSG grundsätzlich zulässig**, kann das Anlegen solcher Dossiers doch auch auf elektronischem Weg erfolgen.

Der Vollständigkeit halber sei in diesem Zusammenhang noch bemerkt, dass mit dem Rückgriff auf das **KiSS** grundsätzlich wohl **kein Abrufverfahren** im Sinne des Art. 19 Abs. 3 DSG einhergeht, dessen Einrichtung in Bezug auf besonders schützenswerte Personendaten eine ausdrückliche formell-gesetzliche Grundlage erfordert.[50] Denn ein Abrufverfahren ist wohl nur anzunehmen, wenn es um die Bekanntgabe von Daten an Dritte (also an andere Behörden oder an Private) geht.[51] In einem System wie dem KiSS sind die Zugänge jedoch grundsätzlich auf die jeweiligen amtsinternen Stellen beschränkt.

Allerdings ist anzumerken, dass damit nur die grundsätzliche Zulässigkeit der Einrichtung eines Informationssystems wie dem KiSS geklärt ist. Eine andere Frage ist jedoch diejenige danach, ob auch die **konkrete Ausgestaltung und Funktionsweise des KiSS** auf der Grundlage von Art. 6 lit. b KDSG i.V.m. den einschlägigen spezialgesetzlichen Grundlagen zulässig ist. Die Anforderung des Art. 6 lit. b KDSG dürfte sich nämlich nicht nur auf den Grundsatz der Datenbearbeitung, sondern auch auf ihre Ausgestaltung im Einzelnen beziehen. M.a.W. muss die Bearbeitung besonders schützenswerter Personendaten insgesamt „zwingend" zur Erfüllung der gesetzlichen Aufgabe notwendig sein, wobei lediglich eine Erleichterung ihrer Wahrnehmung durch die betreffende Datenbearbeitung (in der Form und dem Umfang, wie sie vorgesehen ist) nicht ausreichend ist.[52] So dürfen z.B. nur diejenigen Daten bearbeitet werden, die im Hinblick auf die Erfüllung der gesetzlichen Aufgabe tatsächlich zwingend relevant sind, oder das Dossier ist nur solange aufzu-

---

[50] Vgl. für die Bundesebene Art. 19 Abs. 3 DSG, für die kantonale Ebene z.B. Art. 8a Abs. 5 SHG. Die Notwendigkeit einer gesetzlichen Grundlage in einem solchen Fall dürfte sich aber auch bereits aus den allgemeinen Grundsätzen des Gesetzmässigkeitsprinzips ergeben.

[51] Zum Begriff des Abrufverfahrens im Einzelnen *Epiney/Schleiss*, Jusletter v. 7.11.2011, Rn. 12 ff.

[52] S. schon oben C.II.1.b)bb).

bewahren, wie dies zur Erfüllung des gesetzlichen Auftrages zwingend notwendig ist. Deutlich wird damit auch, dass sich die aus Art. 6 lit. b KDSG ergebenden Anforderungen teilweise mit den allgemeinen Grundsätzen der Zweckbindung und der Verhältnismässigkeit überschneiden (wenn auch die Anforderungen des Art. 6 li. b KDSG teilweise strenger ausgestaltet sind).[53]

Ob und inwieweit diesen Anforderungen im Zusammenhang mit dem **KiSS im Einzelnen Rechnung getragen** wird, muss an dieser Stelle **offen gelassen** werden, da diese Frage nur unter genauer Analyse der im Einzelfall vorgesehenen Funktionsweise des Systems beantwortet werden kann, die aber ihrerseits je nach dem Kontext unterschiedlich sein kann und wohl auch ist. Eine abschliessende und umfassende Beurteilung des KiSS in diesem Sinn implizierte m.a.W. letztlich nicht nur eine eingehende Erörterung der zahlreichen Aufgaben der involvierten Behörden, sondern auch eine eingehende Analyse des Informationssystems selbst (insbesondere auch seiner Inhalte), die im vorliegenden Rahmen nicht geleistet werden kann. Vielmehr kann in diesem Rahmen lediglich der Aspekt der Zugriffsberechtigung etwas vertiefter berücksichtigt werden.[54]

Nur am Rande sei in diesem Zusammenhang aber auch darauf hingewiesen, dass es das Beispiel des KiSS auch zeigt, dass eine **gesetzliche Verankerung** solcher Informationssysteme grundsätzlich sehr sachdienlich, wenn nicht gar verfassungsrechtlich gefordert ist:[55] Denn die Frage, unter welchen Voraussetzung eine bestimmte Bearbeitung besonders schützenswerter Personendaten zur Erfüllung des gesetzlich formulierten Zwecks nun wirklich „zwingend" erforderlich ist, ist nicht immer einfach zu entscheiden und nichtsdestotrotz von grosser Relevanz für die Persönlichkeitsrechte der Betroffenen, und es erscheint vor dem Hintergrund des Gesetzmässigkeitsprinzips insofern bedenklich, die hier zu treffenden Entscheidungen der Verwaltung zu überantworten. Eine klare gesetzliche Regelung, die auf die genauen Bearbeitungszwecke Bezug nimmt, den Umfang der Datenbearbeitung, die an der Datenbearbeitung Beteiligten, die Kategorien der bearbeiteten Daten sowie die Dauer der Datenaufbewahrung bzw. die Voraussetzungen der Löschung der Daten definiert, erschiene hier sowohl in Bezug auf die Rechte der Betroffenen und eine gewisse Transparenz als auch die Wah-

---

53 S. schon oben C.II.1.b)bb).

54 S. sogleich C.II.2.b).

55 Wie bereits erwähnt (oben C.I.), sind die allgemeinen datenschutzrechtlichen Grundsätze (vgl. Art. 4 DSG, Art. 5 KDSG) letztlich Ausprägungen bzw. Konkretisierungen der bereits in der Verfassung (Art. 13 Abs. 2 BV) und der EMRK (Art. 8 EMRK) enthaltenen Vorgaben, vgl. in Bezug auf die gesetzliche Grundlage auch BGE 122 I 360, E. 5.b)dd).

rung der Prärogative des Gesetzgebers zumindest sinnvoll, wenn nicht gar verfassungsrechtlich geboten.

b) Zur Frage der Reichweite der Zugriffsberechtigung

Nach dem Gesagten muss auch die Art und Weise der Datenbearbeitung zur Erfüllung der gesetzlichen Aufgabe „zwingend" im Sinne des Art. 6 lit. b KDSG erforderlich sein, so dass auch die **Ausgestaltung der Zugriffsberechtigung** zwingend zur Erfüllung der **gesetzlichen Aufgaben (zwingend) notwendig** sein muss.[56] Dies betrifft auch – und hierauf beschränken sich die folgenden Ausführungen – die Frage, welche Stellen auf welches (Personen-) Dossier in welchem Modul Zugangsberechtigung haben dürfen.

Ausgangspunkt ist der **Grundsatz**, dass der Zugang zu den jeweiligen Personendaten der Betroffenen nur soweit gewährt werden darf, wie dies zur Erfüllung der erwähnten[57] gesetzlichen Aufgaben zwingend erforderlich ist, so dass nur denjenigen **Personen bzw. Stellen** eine **Zugangsberechtigung** zu gewähren ist, die tatsächlich in **Bezug auf die betroffene Person die gesetzlichen Aufgaben wahrnehmen** (in dem sie diese z.B. betreuen, ihre Sozialhilfebedürftigkeit abzuklären haben oder administrative Unterstützungsarbeit leisten). Im Übrigen impliziert die „zwingende" Erforderlichkeit auch, dass der **Zugang soweit wie möglich** – in Bezug auf die Zahl der zugangsberechtigten Personen – **einzuschränken** ist.

Auf dieser Grundlage können – im Hinblick auf die von Art. 6 lit. b KDSG geforderte „zwingende" Erforderlichkeit – folgende **Leitlinien für eine rechtmässige Ausgestaltung des Zugangs** zu den „Personendossiers" formuliert werden:

- Zugangsberechtigt müssen bzw. dürfen jedenfalls die für die „**Betreuung" der jeweiligen Personen zuständigen Mitarbeitenden bzw. Stellen** der Ämter sein.
- Im Hinblick auf eine effektive (nicht nur effiziente) Wahrnehmung der gesetzlichen Aufgaben kann dies in der Regel nicht nur eine Person bzw. eine Stelle sein, sondern geboten und zulässig ist auch der **Zugang zu den Dossiers durch mehrere Personen**. Nur auf diese Weise kann dem Umstand Rechnung getragen werden, dass es in den Ämtern Teilzeitbeschäftigte gibt und die Betreuung im Übrigen auch im Krankheitsfall oder bei einem Urlaub sichergestellt werden muss.

---

[56] S.o. C.II.1.b)bb), II.2.a).
[57] Oben C.II.2.a).

Allerdings ist die **Zahl der Zugangsberechtigten** vor dem Hintergrund der geforderten „zwingenden“ Erforderlichkeit der Datenbearbeitung **möglichst gering** zu halten. Insofern wäre z.B. zumindest näher zu prüfen, ob in allen Sektionen zwingend immer allen Mitarbeitenden ein Zugriffsrecht gerade auf die F-Module gewährt werden muss, was letztlich von der Grösse der einzelnen Sektionen und der von den einzelnen Mitarbeitenden wahrgenommenen Aufgaben abhängt.

– Auch kann es notwendig sein, dass ein **„Pikettdienst“** – der für Notfälle zuständig ist – **Zugang zu allen Dossiers** hat, da nur auf diese Weise ausserhalb der ordentlichen Arbeitszeiten Notfälle betreut werden können. Allerdings würde sich hier wohl eine **zeitliche Beschränkung** aufdrängen, trägt diese Erwägung doch nur während der Wahrnehmung des Pikettdienstes.
– Nicht ersichtlich ist, dass es zur Erfüllung der gesetzlichen Aufgaben zwingend notwendig ist, dass allgemein **(sonstige) zentrale und / oder administrative Dienste** Zugang zu den Dossiers haben.

  So könnte z.B. eine korrekte Postzuteilung durch die hierfür zuständigen Stellen bzw. Personen wohl ohne einen Zugang zum gesamten Personendossier sichergestellt werden. Dies gilt auch für den Empfang, der die Betroffenen erstmals aufnimmt und an die zuständigen Mitarbeitenden weiterverweist. Es ist nicht ersichtlich, warum hier ein umfassender Zugang zu allen Dossiers notwendig ist; geht es um „gefährliche“ Klienten, so drängte sich eine entsprechende Kennzeichnung, z.B. im Basismodul, auf, in dem auch die zuständigen Personen vermerkt werden könnten, so dass ein Zugang zum Basismodul ausreichen sollte.
– Soweit Teile eines Amtes mit **buchhalterischen und / oder „finanziellen“ Aufgaben** (Revisionen, Berechnungen finanzieller Beiträge, o.ä.) betraut sind, erscheint es zumindest nicht grundsätzlich notwendig, dass diese Stellen als solche umfassend und spontan Zugang zu den Dossiers haben, da jedenfalls einige Aufgaben wohl auch ohne die Kenntnis des vollständigen Dossiers bzw. Moduls wahrgenommen werden können.
– Soweit die konkrete Betreuung bzw. Administration von „Klienten“ auf verschiedene Sektionen eines Amtes (in dem jeweils mehrere Personen tätig sind) verteilt ist, erscheint es **nicht zwingend erforderlich**, dass ein **sektionsübergreifender Zugang zu den Dossiers** gewährt wird, ist doch nicht ersichtlich, warum dies für die Betreuung der Betroffenen zwingend notwendig sein

soll, können doch möglicherweise erforderliche Stellvertretungen grundsätzlich innerhalb einer Sektion organisiert werden; bei gleichwohl möglicherweise (ausnahmsweise) auftretenden Engpässen könnte im Einzelfall Zugang gewährt werden.
Daher wäre aus datenschutzrechtlicher Sicht wohl eine **personalisierte bzw. auf die jeweiligen „Klienten" zugeschnittene Zugriffsrechtematrix** notwendig, die es ermöglichte, die sektionen- bzw. abteilungsübergreifenden Zugriffsrechte zu vermeiden (zumal derartige Zugriffsrechte je nach genauer Ausgestaltung auch dazu führen können, dass Mitarbeitende, die nicht in dem entsprechenden abteilungsübergreifenden Team sind, auf Daten von Personen Zugriff haben, für die sie nicht zuständig sind). In Konstellationen, in denen gewisse Sektionen bzw. Abteilungen zu klein sein sollten, könnte mit im Einzelfall zu gewährenden **Gastrechten bzw. Notfallzugriffen** gearbeitet werden, die ggf. zeitlich zu begrenzen wären.[58]

– Ganz allgemein vermag allein eine gewisse **(administrative) Vereinfachung der Tätigkeit der Behörde** eine **Zugangsberechtigung** bzw. deren Erweiterung **nicht zu begründen**, würde damit doch dem Erfordernis der „zwingenden" Erforderlichkeit der Datenbearbeitung für die Wahrnehmung der gesetzlichen Aufgabe nicht Rechnung getragen. Damit reicht **eine reine „Sachdienlichkeit" der Datenbearbeitung nicht aus**, sondern es ist darzulegen, dass ohne diese die Erfüllung der gesetzlichen Aufgabe geradezu vereitelt würde.[59]
Daher ist ggf. – statt eines generalisierten Zugangs einer bestimmten Sektion oder eines Teils eines Amtes zu einem Dossier – eine **einzelfallweise Übermittlung von Daten** auf Anfrage oder auf Initiative eines Zugangsberechtigten in Betracht zu ziehen, die sich im Übrigen ggf. auf die konkret notwendigen Angaben beschränken kann (z.B. gewisse Angaben über die finanzielle Situation einer Person, unter Aussparung sonstiger, z.B. im Fallführungs-Modul enthaltener Informationen).
Effizienzgesichtspunkte können allenfalls in Ausnahmefällen (möglicherweise wenn z.B. der Personalbestand des Amtes an-

---

[58] Vgl. zum Vorschlag, die Gastrechte (bei einem Informationssystem eines Spitals) auf 12 Stunden zu beschränken, Décision de la Commission cantonale de la protection des données du 23 février 2000 dans la procédure relative aux fichiers informatisés des données médicales des hôpitaux jurassiens, E 3.e)

[59] S.o. C.II.1.b)bb).

sonsten spürbar erhöht werden müsste und dies auch nicht durch eine andere interne Organisation vermieden werden könnte) dazu führen, dass die Erfüllung des gesetzlichen Zwecks verunmöglicht würde. Hingegen reicht allein eine gewisse Arbeitserleichterung (z.B. eine gewisse Beschleunigung bestimmter Abläufe oder das Vermeiden von Anfragen oder Übermittlungen im Einzelfall) keinesfalls aus.

– Sodann ist generell auch immer danach zu fragen, ob nicht **eingeschränkte Zugangsrechte bzw. ein teilweiser Zugang** oder **Zugänge bzw. bestimmte Datenübermittelungen im Einzelfall** für die Wahrnehmung der gesetzlichen Aufgabe ausreichend sein könnten. Ebenso ist ggf. (z.B. bei (nur) für bestimmte Zuweisungen zuständigen Stellen) zu prüfen, ob ein **zeitlich beschränkter Zugang** ausreichend sein kann.

  Eine weitere Konkretisierung bzw. Einschränkung der Zugriffsrechte könnte sodann erfolgen, indem festgelegt wird, welche (Abteilung oder) Mitarbeiterin berechtigt ist, Personendaten in einem Modul (nur) zu lesen oder auch zu bearbeiten (bspw. ergänzen, korrigieren, löschen usw.).[60]

– Schliesslich ist die Ausgestaltung der Zugriffsrechte grundsätzlich für den Fall, dass **Dossiers wegen des Wegfalls einer Massnahme geschlossen** (und ggf. archiviert) werden, anders bzw. enger zu definieren. Jedenfalls gleich weite Zugriffsrechte wie bei der Bearbeitung erscheinen hier grundsätzlich nicht zwingend erforderlich. Auch ganz allgemein ist der Umgang mit Daten, die Personen betreffen, deren Dossier abgeschlossen ist, klar zu regeln.

III. Zum Grundsatz der Zweckbindung

Nach dem auch in Art. 5 Abs. 2, 4 KDSG[61] verankerten **Grundsatz der Zweckbindung** dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.[62]

---

[60] Vgl. als Beispiel die Anhänge der Verordnung über die Harmonisierung amtlicher Register vom 12.3.2008, BSG 152.051.

[61] S. auch Art. 4 Abs. 3 DSG.

[62] Vgl. zum Grundsatz der Zweckbindung, m.w.N., *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 29 ff.; *Meier*, Protection des données, § 4, Rn. 716 ff.

In Bezug auf die Einrichtung und den Betrieb des KiSS bedeutet dieser Grundsatz, dass die in diesem Rahmen erfolgende Datenbearbeitung nur zu dem **gesetzlich vorgesehenen Zweck** (z.B. im Bereich der Sozialhilfe bzw. des Kindes- und Erwachsenenschutzes) erfolgen darf. Grundsätzlich ist davon auszugehen, dass diesem Erfordernis entsprochen wird bzw. unproblematisch entsprochen werden kann.

IV. Zum Grundsatz der Verhältnismässigkeit

Bei der **Verhältnismässigkeit** handelt es sich um einen rechtsstaatlichen Grundsatz, der bereits aus Art. 5 Abs. 2 BV und (für den Datenschutz) aus Art. 8 Abs. 2 EMRK und Art. 5 lit. c DSK abgeleitet werden kann und demzufolge auch im kantonalen Datenschutzrecht Geltung haben muss.[63] So nimmt auch Art. 5 Abs. 3 KDSG auf diesen Grundsatz Bezug.[64] Das Verhältnismässigkeitsprinzip ist aufgrund seiner Verankerung in den verfassungsrechtlichen Persönlichkeitsrechten und seiner Konkretisierung durch die (kantonalen) Datenschutzerlasse bei jeder Bearbeitung persönlichkeitsrelevanter Daten zu beachten, so dass dieser Grundsatz auch auf die **behördeninterne Weitergabe von Personendaten** anwendbar ist.[65]

Weiter ist auch hier[66] zu betonen, dass der Verhältnismässigkeitsgrundsatz jedenfalls einzuhalten ist und hierfür allein die ihm zu entnehmenden Anforderungen von Bedeutung und zu beachten sind, so dass es für die Prüfung der Verhältnismässigkeit – jedenfalls soweit Geeignetheit und Erforderlichkeit betroffen sind – irrelevant ist, ob die Bearbeiter von Personendaten (gesetzlichen) Schweigepflichten oder Amtsgeheimnissen unterliegen. Allenfalls im Rahmen der Verhältnismässigkeit i.e.S. könnte in Erwägung gezogen werden, diesen Aspekt zu berücksichtigen.

Die Bearbeitung von Personendaten muss somit zum einen **geeignet** und **erforderlich** sein, m.a.W. den (mit dem öffentlichen Interesse) angestrebten Zweck mit Hilfe des mildesten Mittels so präzise wie möglich erreichen. Zum anderen müssen die involvier-

---

63 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 23; vgl. ferner z.B. Art. 28 Abs. 3 BV-BE bei der Einschränkung von Grundrechten.

64 S. im Übrigen auch Art. 18 Abs. 2 BV-BE. Vgl. zum Verhältnismässigkeitsprinzip im kantonalen Datenschutzrecht *Waldmann/Oeschger*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, Rn. 64 f.

65 Vgl. (zu öffentlich-rechtlichen Krankenhäusern) *Baeriswyl*, in: Datenschutz im Gesundheitswesen, 49 (60).

66 Vgl. im Zusammenhang mit Art. 6 lit. b KDSG auch schon oben C.II.1.b)bb).

ten öffentlichen und privaten Interessen gegeneinander abgewogen werden und im Resultat in einem angemessenen, bzw. vernünftigen Verhältnis zueinander stehen (**Verhältnismässigkeit i.e.S.**). Eine Verhältnismässigkeitsprüfung hat – auch wenn eine gesetzliche Grundlage und ein öffentliches Interesse einschlägig ist – sodann immer objektiv und im Einzelfall für den konkreten Sachverhalt zu erfolgen.[67]

Soweit die **Geeignetheit** und **Erforderlichkeit** betroffen sind, ist daran zu erinnern, dass es im vorliegenden Zusammenhang um eine Datenbearbeitung geht, die auf **Art. 6 lit. b KDSG** gestützt ist und insofern zur Erfüllung der jeweiligen gesetzlichen Aufgabe „zwingend" erforderlich sein muss. Ist diese Voraussetzung erfüllt, ist davon auszugehen, dass (erst recht) auch denjenigen der Geeignetheit und der Erforderlichkeit entsprochen wurde, so dass insoweit auf die obigen Ausführungen verwiesen werden kann.[68]

Bei der Verhältnismässigkeit i.e.S. geht es – wie erwähnt – um eine **umfassende Abwägung der involvierten Interessen**, die im Einzelfall zu erfolgen hat. Ohne Anspruch auf Vollständigkeit seien hier die im Zusammenhang mit der Errichtung und dem Betreiben eines Informationssystems wie dem KiSS jedenfalls in die Überlegungen einzubeziehenden Interessen kurz erwähnt, wobei zwischen denjenigen Interessen, die für einen „strengen" Datenschutz (und damit in vorliegendem Zusammenhang eine möglichst weitgehende Beschränkung des Zugangs zu den in KiSS enthaltenen Personendaten) angeführt werden können, und denjenigen, die (zusätzliche) Eingriffe in die Persönlichkeitsrechte der Betroffenen rechtfertigen könnten, zu unterscheiden ist:

– Zunächst ist selbstredend die **Intensität des Eingriffs in die Persönlichkeitsrechte der Betroffenen** zu eruieren, die von verschiedenen Elementen, so insbesondere Art und Umfang der über sie gespeicherten Daten, der Reichweite der Zugriffsberechtigung auf diese, aber auch den ergriffenen technischen und organisatorischen Massnahmen (die die Datensicherheit positiv beeinflussen und somit potenzielle Persönlichkeitsverletzungen bei der Bearbeitung von Personendaten verringern),[69] abhängt,[70] wo-

---

[67] *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 24, 27, m.w.N.; *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 60 f. Vgl. ferner etwa BGE 136 I 87, E. 3.2.

[68] S.o. C.II.II.2.b).

[69] Und daher bei der Interessenabwägung ebenfalls zu berücksichtigen sind, vgl. etwa *Meier*, Protection des données, Rn. 793; EGMR, Urt. v. 17.7.2008, No.

bei im vorliegenden Zusammenhang selbstredend auch zu berücksichtigen ist, dass es um besonders schützenswerte Personendaten geht, deren Bearbeitung grundsätzlich „schwerer" wiegt. Daneben und darüber hinaus stellt **Datenschutz auch ein öffentliches Interesse** dar.[71] Ferner haben Einrichtungen, insbesondere solche, die in sozialen Nahbereichen „Dienstleistungen" anbieten (bspw. Spitäler, Sozialhilfedienste usw.), auch ein Interesse daran, die Privatsphäre ihrer Klienten zu schützen, um ihre Vertrauenswürdigkeit gegenüber denselben zu wahren.[72]

– Die **Erfüllung der gesetzlichen Aufgaben** – wie das **Funktionieren des Erwachsenen- und Kindesschutzes sowie der Sozialhilfe** – stellt das wesentliche öffentliche Interesse an der Datenbearbeitung und damit dem Eingriff in die Persönlichkeitsrechte der Betroffenen dar.[73] Auch ist die staatliche Pflicht, seine

---

20511/03 (I/Finnland), Rn. 38: „The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention […]."

70 Vgl., mit Bezug zur EMRK, *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 17, m.w.N: „Der Gerichtshof legt hier bei der Gewichtung der in Frage stehenden Interessen sowie der Prüfungsdichte im Rahmen der Analyse der einzelnen Merkmale der Verhältnismässigkeit je nach den betroffenen öffentlichen Interessen und der Schwere des Eingriffs in die Privatsphäre unterschiedliche Massstäbe an." Vgl. ferner zu dieser Gewichtung bei der Weitergabe von Personendaten schon Entscheid des Regierungsrates Nr. 2020 vom 23. Mai 1984, Gemeinde Bern und Ostermundigen gegen Direktion für Verkehr, Energie und Wasser, E. 4.c).

71 Vgl. BGE 138 II 346, E. 10.1; BGE 136 II 508, E. 6.3.2. S. hierzu auch *Epiney*, in: Datenschutz in Europa und die Schweiz, 1 (7 f.).

72 Vgl. *Mösch Payot*, Datenschutz im Sozialbereich, 109 (111, 116 f.); *Baeriswyl*, in: Datenschutz im Gesundheitswesen, 49 (65), der (auf einer organisatorischen Ebene bei öffentlich-rechtlichen Krankenhäusern) von einem Qualitätsmerkmal spricht; s. auch EGMR, Urt. v. 17.7.2008, No. 20511/03 (I/Finnland), Rn. 38; EGMR, Urt. v. 25.2.1997, RJD 1997-I (Z./Finnland), Rn. 95 f.; Décision de la Commission cantonale de la protection des données du 23 février 2000 dans la procédure relative aux fichiers informatisés des données médicales des hôpitaux jurassiens, E. 2.a): „Ce droit protège la sphère privée du patient et constitue la condition nécessaire à l'établissement d'une relation de confiance avec le soignant ; il contribue aussi au bon exercice de la profession médicale." Ferner *Rosch*, in: Menschenrechte und Digitalisierung, 261 (262 f.).

73 Aus diesem Interesse lassen sich weitere Argumente ableiten, welche von Behörden im Rahmen einer Interessensabwägung vorgebracht werden können, wobei insbesondere das öffentliche Interesse, dass „Sozialhilfe nicht aufgrund tatsachenwidriger oder unvollständiger Information zu Unrecht

Bürgerinnen und Bürger (und damit auch seine Angestellten) mit den nach den Umständen angemessenen Massnahmen vor Eingriffen anderer Privater in ihr Recht auf Leben und körperliche Gesundheit zu schützen, einzubeziehen, was etwa impliziert, dass gewisse Daten über (potentiell) gefährliche „Klienten" der Sozialdienste intern erweitert ausgetauscht werden können. Effizienzargumenten der Verwaltung kann im vorliegenden Zusammenhang hingegen wohl nur ein geringes Gewicht zukommen, geht es doch um grundsätzlich weitgehende Eingriffe in die Persönlichkeitsrechte der Betroffenen.

In Bezug auf das KiSS wäre demnach zu prüfen, ob die Bearbeitung der besonders schützenswerten Personendaten – die zwingend für die Erfüllung der gesetzlichen Aufgaben ist bzw. sein muss[74] – und damit der hiermit verbundene **Eingriff in die Persönlichkeitsrechte** der Betroffenen insgesamt auch in einem **angemessenen Verhältnis** zu den mit der Art und Weise der Datenbearbeitung verfolgten **gesetzlichen Zielsetzungen** steht, wobei in verfassungskonformer Auslegung auch andere Aspekte (insbesondere Anliegen des Schutzes von Leib und Leben von Mitarbeitern) berücksichtigt werden können. Da im Zusammenhang mit Art. 6 lit. b KDSG bereits zu prüfen ist, ob die Datenbearbeitung zur Erreichung des gesetzlichen Ziels zwingend erforderlich ist, geht es hier darum, ob die Datenbearbeitung auch den Anforderungen der Angemessenheit genügt. Diese Prüfung kann – wie bereits erwähnt – nur im Einzelfall unter Berücksichtigung aller relevanten Elemente erfolgen.[75]

Grundsätzlich kann festgehalten werden, dass im Falle der Erfüllung der Voraussetzungen des Art. 6 lit. b KDSG in aller Regel auch die **Angemessenheit** der im Rahmen des KiSS erfolgenden Datenbearbeitung **vertretbar bejaht** werden kann, da es in diesem Rahmen notwendig ist, dass die Datenbearbeitung „zwingend" für den gesetzlichen Zweck erforderlich ist, womit bereits Effizienzerwägungen der Verwaltung grundsätzlich ausgeschlossen sind. Da-

---

ausgerichtet wird" (BGE 138 I 331, E. 7.4.3.1: „Dabei geht es auch um die Bewahrung des Vertrauens des Bürgers in den Staat […]"), hervorzuheben ist.

74 S.o. C.II.2.

75 Vgl. etwa BGE 138 II 346, E. 10.3.: „Im Rahmen der Interessenabwägung sind die konkreten Interessen zu ermitteln, diese mithilfe rechtlich ausgewiesener Massstäbe zu beurteilen und zu optimieren, sodass sie mit Rücksicht auf die Beurteilung, die ihnen zuteil wurde, im Entscheid möglichst umfassend zur Geltung gebracht werden können[…]."

her kann die Angemessenheit nur dann verneint werden, wenn die konkrete Art der Datenbearbeitung in keinem Verhältnis mehr zu dem gesetzlich verfolgten Zweck steht, was z.B. dann denkbar ist, wenn mit einer gesetzlich vorgesehenen Berichterstattung sehr gewichtige Eingriffe in die Persönlichkeitsrechte der Betroffenen verbunden sind.

V. Sonstige Vorgaben

Die kantonalen Datenschutzgesetze – so auch das Datenschutzgesetz des Kantons Bern – enthalten noch eine Reihe **weiterer Vorgaben**, die beim Umgang mit Personendaten zu beachten sind. Einige wenige, in unserem Zusammenhang besonders relevante, sollen nachfolgend kurz skizziert werden, nämlich die Datensicherheit (1.), die Protokollführung (2.) sowie die Vorabkontrolle (3.).

1. Datensicherheit (Art. 17 KDSG, Art. 4 f. DSV)

Das Gesetz äussert sich zur Datensicherung nur sehr rudimentär, indem es die verantwortliche Behörde (Art. 2 Abs. 6, 8 KDSG) dazu anhält, für die geeigneten technischen, organisatorischen und administrativen Massnahmen zur Sicherung der Personendaten zu sorgen (Art. 17 KDSG). Der Regierungsrat des Kantons Bern hat die Bestimmung mit den Art. 4 ff. DSV näher konkretisiert. Neben den grundsätzlich zu erfüllenden Massnahmen (Art. 4 DSV) finden sich in Art. 5 DSV besondere Massnahmen, die die verantwortliche Behörde insbesondere bei der elektronischen Bearbeitung von Personendaten zu treffen hat.

Art. 4 f. DSV wurden – mit wenigen Ausnahmen – aus der VDSG übernommen (vgl. Art. 8 ff. i.V.m. Art. 20 VDSG). Es rechtfertigt sich insofern, die Lehre zu Art. 9 Abs. 1 lit. g und h VDSG beizuziehen, welcher wortwörtlich mit Art. 5 Abs. 2 lit. g und h DSV übereinstimmt.

Im vorliegenden Zusammenhang ist insbesondere Art. 5 Abs. 1 lit. g DSV von Interesse, welcher die **Zugriffskontrolle** der berechtigten Personen reglementiert, wenn die verantwortliche Behörde ein Datenkommunikationsnetz zur Verfügung stellt.[76] Die Bestim-

[76] Art. 4 DSV: Die Systeme sind insbesondere gegen die Risiken der unbefugten oder zufälligen Vernichtung, des zufälligen Verlusts, der technischen Fehler, der Fälschung, des Diebstahls oder der widerrechtlichen Verwendung

mung setzt voraus, dass der Zugriff der berechtigten Personen auf diejenigen Personendaten zu beschränken ist, die sie für die Erfüllung ihrer Aufgabe benötigen. Die Bestimmung ist – soweit ersichtlich – sowohl auf behördeninterne als auch auf behördenexterne Datenkommunikationsnetze anwendbar, sofern diese (datenschutz-)rechtlich zulässig sind.

Konsequenterweise müssen aufgrund der Zugriffskontrolle auch die berechtigten Personen (durch das Datenkommunikationsnetz) identifiziert werden und unberechtigten Personen der Zugang zum System verweigert werden können, was insofern auch eine Protokollierung der Zugriffe[77] voraussetzen würde.[78]

Insgesamt haben die – im Einzelfall – zu implementierenden (technischen und organisatorischen) Massnahmen dem Grundsatz der **Verhältnismässigkeit** zu entsprechen und sich gegenseitig zu ergänzen bzw. nicht gegenseitig zu behindern.[79] Die Massnahmen sollen m.a.W. angemessen sein und insbesondere im Hinblick auf den Zweck, die Art und den Umfang der Datenbearbeitung, die potenziellen Risiken für die betroffenen Personen und den gegenwärtigen Stand der Technik ausgestaltet werden (Art. 4 Abs. 2 DSV).[80] Diese Aspekte kommen in Art. 5 Abs. 1 lit. g DSV besonders zum Ausdruck, wonach den berechtigten Personen der Zugriff nur unter der Voraussetzung erlaubt werden darf, dass die Bearbeitung der Personendaten für die Erfüllung ihrer Aufgaben erforderlich und notwendig ist.

Zweck der Implementierung dieser Begrenzung des Zugangs auf ein behördeninternes Kommunikationsnetz ist die Verringerung der

---

und gegen das unbefugte Ändern, Kopieren oder andere unbefugte Bearbeitungen von Personendaten zu schützen.

77 Hierzu auch noch unten C.V.2.

78 Dies erinnert an die Bekanntgabekontrolle (Art. 5 Abs. 1 lit. d DSV) und die Benutzerkontrolle (Art. 5 Abs. 1 lit. f DSV). Zur Protokollierung, vgl. unten C.V.2.

79 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 53, 57; *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 18 f., der von „Kontrollzielen" spricht, die unter dem Vorbehalt der Verhältnismässigkeit zu implementieren sind. Ferner *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 3; *Meier*, Protection des données, Rn. 782, 790, 800: „Nul ne prétend pouvoir jamais atteindre la sécurité absolue. Mais l'absence de sécurité ou des mesures insuffisantes constituent une violation de la LPD."

80 Auch die Kosten einer Implementierung können miteinbezogen werden, allerdings nur zweitrangig. Vorgesehen ist dies in Art. 17 Abs. 1 RL 95/46. Vgl. *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 3; *Meier*, Protection des données, Rn. 792.

Gefahr der bewussten oder unbewussten Fehlbearbeitung sowie die Prävention von Datenmissbrauch.[81] Sachdienlich für die im konkreten Fall zu implementierenden **Autorisierungsmechanismen** erscheinen folgende Massnahmen, wobei deren Verhältnismässigkeit jeweils im Einzelfall zu prüfen ist:[82]

– differenzierte Zugangsrechte für jede Mitarbeiterin und jeden Mitarbeiter der Behörde, welche die Bearbeitungsmöglichkeiten, die zeitliche Beschränkung, Filter usw. festlegen (rollenbasierte Zugriffsbeschränkung);
– Erarbeitung einer Zugangsrechtematrix;
– eindeutige Authentifizierung beim Zugang zum Kommunikationsnetz mit ausreichender Sicherheit (Passwort) im Hinblick auf die potenziellen Risiken der Datenbearbeitung (besonders schützenswerte Personendaten);
– Protokollierung der Zugriffe auf das Kommunikationsnetz.[83]

Behördenintern ist u.E. ein **Datenbearbeitungsreglement** erforderlich. Das KDSG sieht ein solches – im Gegensatz zum Bundesrecht (Art. 21 VDSG, für öffentliche Organe)[84] – nicht vor. Ein solches zu erstellen dürfte sich allerdings aus verschiedenen Gründen – zumindest bei Behörden, die besonders schützenswerte Personendaten bearbeiten[85] – aufdrängen: Hierfür sprechen Gründe der Praktikabilität, um die Organisationsstrukturen der Behörden mit den Zugriffsmechanismen abzustimmen, ebenso wie Erwägungen der Rechenschaft und Transparenz[86] gegenüber den Betroffenen, da mit

---

81 EDÖB, Technische und organisatorische Massnahmen, ein Leitfaden, September 2011, 12.

82 Vgl. EDÖB, Technische und organisatorische Massnahmen, ein Leitfaden, September 2011, 13; *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 19; *Meier*, Protection des données, Rn. 807 („règle du „need-to-know“).

83 Vgl. hierzu unten C.V.2.

84 Vgl. hierzu EDÖB, Technische und organisatorische Massnahmen, ein Leitfaden, September 2011, 30 f.; *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 21 ff.; *Meier*, Protection des données, Rn. 815 ff. (Privatpersonen).

85 Bundesorgane sind zur Erstellung eines Reglements verpflichtet, wenn sie (unter anderem) besonders schützenswerte Personendaten bearbeiten (Art. 21 Abs. 1 lit. a VDSG).

86 EDÖB, Technische und organisatorische Massnahmen, ein Leitfaden, September 2011, 30: „Mit einem solchen Reglement soll die Transparenz sichergestellt werden, die für die Erarbeitung und die Verwaltung einer Personendatensammlung (Sammlung) notwendig ist.“ Interessierte wären grundsätzlich berechtigt, das Reglement aufgrund des Informationsgesetzes einzuse-

der Bearbeitung von besonders schützenswerten Personendaten (schwerwiegende) Verletzungen der Persönlichkeit einhergehen können. Auch kann auf diese Weise der Nachweis von Verletzungen der Zugriffsrechte erleichtert werden.[87]

Unter den gegebenen Voraussetzungen wären im Hinblick auf die Regelung der Zugriffskontrolle u.E. insbesondere folgende Aspekte in ein Bearbeitungsreglement aufzunehmen, wobei als Orientierung die Anforderungen an Bearbeitungsreglemente von Bundesorganen beigezogen werden können (Art. 21 Abs. 2 VDSG):

– die Beschreibung der einzelnen Datenfelder und die Organisationseinheiten, die darauf Zugriff haben, m.a.W. eine Zugriffsmatrix (Art. 21 Abs. 2 lit. e VDSG);
– die Art (Einsichts-, Bearbeitungs- und Löschungsrechte) und der Umfang (welche Datenfelder) des Zugriffs der einzelnen Benutzer der Datensammlung, wobei dieser (zweite) Aspekt u.E. auch mit ersterem kombiniert werden könnte (Art. 21 Abs. 2 lit. f VDSG);
– eine allgemeine Umschreibung der Kontrollverfahren betreffend die Zugriffe der einzelnen Benutzer der Datensammlung (Art. 21 Abs. 2 lit. d VDSG).

hen. Vgl. Art. 27 Abs. 1 IG (Gesetz über die Information der Bevölkerung vom 1.11.1993, BSG 107.1).

87 EDÖB, Technische und organisatorische Massnahmen, ein Leitfaden, September 2011, 15.

2. Protokollierung (Art. 17 KDSG, Art. 6 DSV)

Art. 6 DSV (i.V.m. Art. 17 KDSG) – welcher mit wenigen Ausnahmen Art. 10 VDSG entspricht – verpflichtet die verantwortliche Behörde zur **Protokollierung** einer **automatisierten Bearbeitung von besonders schützenswerten Personendaten** oder von Personendaten, die einer besonderen Geheimhaltungspflicht unterstehen (Art. 6 Abs. 1 DSV). Im Sinne einer Abschwächung dieser Pflicht und der Verhältnismässigkeit besteht die Pflicht nur, wenn präventive Massnahmen den Datenschutz nicht gewährleisten können. Eine Konkretisierung erfährt die Pflicht in Art. 6 Abs. 2 DSV, der der Behörde eine Protokollierungspflicht insbesondere dann auferlegt, wenn sonst keine andere Möglichkeit besteht, nachträglich festzustellen, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden. Die Protokolle sind ferner während eines Jahres revisionsgerecht aufzubewahren und sind ausschliesslich denjenigen Stellen zugänglich zu machen, denen die Überwachung der Datenschutzvorschriften obliegt (Art. 6 Abs. 3 DSV).

Zu protokollieren wären im Hinblick auf die oben erwähnten Massnahmen somit grundsätzlich sämtliche Zugriffe der zur Bearbeitung berechtigten Personen bzw. Mitarbeiterinnen und Mitarbeiter der Behörde in sog. *„log files"*. Sie sind zudem während einem Jahr aufzubewahren.

Die Protokollpflicht wird in der Lehre zum Datenschutzrecht des Bundes (für Privatpersonen) aufgrund des damit einhergehenden „enormen Aufwandes" teilweise als praxisfremd und inkonsequent umschrieben.[88] Der Pflicht werde kaum nachgelebt und auch die rechtlichen Folgen einer Nichtbeachtung würden aus Perspektive der Verpflichteten regelmässig als vernachlässigbar eingestuft.

---

[88] Vgl. *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 10, 20. Ferner *Meier*, Protection des données, Rn. 814: „Cette mesure ne doit pas être idéalisée. En effet, elle peut se révéler extrêmement lourde en termes de ressources humaines et techniques […]." Er bringt folgende Argumente gegen die Protokollpflicht vor: Das Protokoll sage nichts darüber aus, wieso die Datenbearbeitung vorgenommen wurde. Es bringe Aussenstehenden nicht viel, da eine vertiefte Kenntnis des Informatiksystems vorausgesetzt werde, um das Protokoll zu verstehen. Das Protokoll enthalte keine Informationen über die physische Sicherheit (wenn bspw. jemand rechtmässig Personendaten bearbeitet und die Informationen dann mündlich weitergibt). Das Protokoll verliere seine präventiven Auswirkungen, wenn die Mitarbeiter davon ausgehen, es werde nur zur rechtlichen Absicherung ohne Konsequenzen bei Nichtbeachtung des Reglements geführt.

Im Sinne der bereits erwähnten Verhältnismässigkeit wird denn auch die Meinung vertreten, dass durch das System von rollenbasierten Zugriffsberechtigungen (oder aufgrund eines Vier-Augen-Prinzips) auf die Protokollierung **verzichtet** werden könne.[89] Diese Meinung ist u.E. aufgrund der Subsidiarität von Art. 6 Abs. 1 DSV vertretbar, wenn sich der Verzicht der Protokollierung lediglich auf die Zugriffe beschränkt, welche aufgrund des Bearbeitungsreglements für spezifische Situationen erlaubt sind.[90]

Im Übrigen ist darauf hinzuweisen, dass die Protokollierung – so sie durchgeführt wird – nichts daran ändert, dass die **Vorgaben der Art. 5, 6 KDSG jedenfalls einzuhalten** sind.

3. Vorabkontrolle (Art. 17a KDSG)

Art. 17a KDSG verpflichtet die zuständige Behörde, im Falle der beabsichtigten Bearbeitung u.a. von besonders schützenswerten Personendaten, diese im Vorfeld der Aufsichtsstelle zur Stellungnahme zu unterbreiten; gleiches gilt für wesentliche Modifikationen solcher Bearbeitungen. Die Aufsichtsstelle gibt zu der beabsichtigten Datenbearbeitung eine Empfehlung im Sinne von Art. 35 Abs. 3 KDSG ab.

Das KiSS erfüllt die Voraussetzungen für das Greifen der Pflicht zur Vorabkontrolle, so dass im Falle eines Rückgriffs auf dieses System eine solche durchgeführt werden muss (was jedoch dann nicht gilt, wenn das KiSS vor Inkrafttreten des Art. 17a KDSG eingeführt wurde). Im Übrigen unterliegt jede ins Gewicht fallende Weiterentwicklung der Vorabkontrolle.

---

[89] Wobei allerdings nicht ganz klar wird, ob die Autoren diese Aussagen auf die privaten Datenbearbeiter beschränken. Vgl. *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 20; *Meier*, Protection des données, Rn. 812. Vgl. ferner EDÖB, Technische und organisatorische Massnahmen, ein Leitfaden, September 2011, 16.

[90] Wäre eine zusätzliche Anpassung gar nicht nötig bzw. ergibt sich die Protokollierung schon aufgrund der bestehenden Informationssysteme, ist diese Meinung allerdings nicht dahingehend zu verstehen, dass diese „Protokolle" vor dem Ablauf eines Jahres gelöscht werden können.

D. Zusammenfassung und Schlussbemerkung

I. Zusammenfassung

Die **Ergebnisse** der Studie können wie folgt thesenartig **zusammengefasst** werden:

- Aus datenschutzrechtlicher Sicht sind für die Errichtung und den Betrieb eines Informationssystems wie das KiSS die **kantonalen Vorgaben** einschlägig, soweit die Datenbearbeitung durch kantonale Behörden erfolgt. Bei der Auslegung des kantonalen Rechts kann auch auf die **entsprechenden Grundsätze des DSG** zurückgegriffen werden, ganz abgesehen davon, dass die Vorgaben der **Verfassung** und der **EMRK** sowieso bei der Auslegung des kantonalen Rechts zu beachten sind.[91]
- **Besonders schützenswerte Personendaten** dürfen nach Art. 6 KDSG lediglich bearbeitet werden, wenn sich zusätzlich zu den allgemeinen Anforderungen nach Art. 5 KDSG die Zulässigkeit aus einer gesetzlichen Grundlage klar ergibt oder die Erfüllung einer gesetzlichen Aufgabe es zwingend erfordert oder die betroffene Person ausdrücklich zugestimmt hat.[92]
- Im Zusammenhang mit dem Klienten-Informationssystem für Sozialarbeit (KiSS) ist davon auszugehen, dass es grundsätzlich um die **Bearbeitung besonders schützenswerter Personendaten** geht.[93]
- In zahlreichen Kantonen – und jedenfalls im Kanton Bern – dürfte keine klare gesetzliche Grundlage für das KiSS bestehen. Von einer ausdrücklichen Zustimmung der Betroffenen kann nicht ausgegangen werden. Daher muss für die Errichtung und den Betrieb des KiSS ein (anderes) Surrogat für eine Rechtsgrundlage bestehen. Im Kanton Bern – wobei die Rechtslage in anderen Kantonen weitgehend parallel ausgestaltet ist – könnte Art. 6 lit. b KDSG einschlägig sein, wonach die Bearbeitung zur Erfüllung einer **gesetzlichen Aufgabe „zwingend" erforderlich** sein muss. Diese Anforderung bezieht sich sowohl auf den **Grundsatz der Bearbeitung** der besonders schützenswerten Personen-

---

91 C.I.
92 C.II.1.
93 C.II.2.a).

daten als auch auf deren genaue **Ausgestaltung** (unter Einschluss der Zugriffsrechte).[94]

- Da das KiSS es den involvierten Behörden ermöglichen soll, ihre gesetzlichen Aufgaben in den Bereichen des Kindes- und Erwachsenenschutzes sowie der Sozialhilfe wahrzunehmen und hierfür notwendigerweise auch besonders schützenswerte Personendaten bearbeitet werden müssen, ist die **Einrichtung eines Informationssystems wie das KiSS nach Art. 6 lit. b KDSG grundsätzlich zulässig**.[95]
- Allerdings muss auch die **konkrete Ausgestaltung und Funktionsweise des KiSS** – insbesondere im Bereich der Zugriffsregelung – auf der Grundlage von Art. 6 lit. b KDSG i.V.m. den einschlägigen spezialgesetzlichen Grundlagen in jeder Beziehung zulässig sein. Art. 6 lit. b KDSG impliziert den **Grundsatz**, dass der Zugang zu den jeweiligen Personendaten der Betroffenen nur soweit gewährt werden darf, wie dies zur Erfüllung der erwähnten gesetzlichen Aufgaben zwingend erforderlich ist, so dass nur denjenigen **Personen bzw. Stellen** eine **Zugangsberechtigung** zu gewährt werden darf, die tatsächlich in **Bezug auf die betroffene Person die gesetzlichen Aufgaben wahrnehmen** (in dem sie diese z.B. betreut oder ihre Sozialhilfebedürftigkeit abzuklären haben). Im Übrigen impliziert die „zwingende" Erforderlichkeit auch, dass der **Zugang soweit wie möglich** – in Bezug auf die Zahl der zugangsberechtigten Personen – **einzuschränken** ist bzw. ggf. ein eingeschränkter Zugang oder ein Zugriff im Einzelfall zu gewähren ist. Auch vermag allein eine gewisse **(administrative) Vereinfachung der Tätigkeit der Behörde** eine **Zugangsberechtigung** bzw. deren Erweiterung **nicht zu begründen**, würde damit doch dem Erfordernis der „zwingenden" Erforderlichkeit der Datenbearbeitung für die Wahrnehmung der gesetzlichen Aufgabe nicht Rechnung getragen.
- Im Übrigen wäre eine **gesetzliche Verankerung** von Errichtung und Betrieb eines Informationssystems wie das KiSS grundsätzlich sehr sachdienlich, wenn nicht gar womöglich verfassungsrechtlich gefordert.[96]
- **Grundsätzlich** kann im Falle der Erfüllung der Voraussetzungen des Art. 6 lit. b KDSG in aller Regel auch die **Angemessenheit**

---

[94] C.II.2.a).
[95] C.II.2.a).
[96] C.II.2.a).

der im Rahmen des KiSS erfolgenden Datenbearbeitung **vertretbar bejaht** werden, da es in diesem Rahmen notwendig ist, dass die Datenbearbeitung „zwingend" für den gesetzlichen Zweck erforderlich ist, womit bereits Effizienzerwägungen der Verwaltung grundsätzlich ausgeschlossen sind. Daher kann die Angemessenheit nur dann verneint werden, wenn die konkrete Art der Datenbearbeitung in keinem Verhältnis mehr zu dem gesetzlich verfolgten Zweck steht, was z.B. dann denkbar ist, wenn mit einer gesetzlich vorgesehenen Berichterstattung sehr gewichtige Eingriffe in die Persönlichkeitsrechte der Betroffenen verbunden sind.[97]

– Das kantonalen Datenschutzgesetze – so auch das Datenschutzgesetz des Kantons Bern – enthalten noch eine Reihe **weiterer Vorgaben**, die beim Umgang mit Personendaten zu beachten sind, wobei in unserem Zusammenhang diejenigen über die Datensicherheit, die Protokollführung sowie die Vorabkontrolle von besonderer Bedeutung sind.[98] Hervorzuheben ist, dass die Errichtung und der Betrieb eines Informationssystems wie das KiSS im Kanton Bern einer **Vorabkontrolle** unterliegt, die auch bei wesentlichen Modifikationen des Systems zum Zuge kommen muss.[99]

II. Schlussbemerkung

Die angestellten Überlegungen konnten aufzeigen, dass den für die Errichtung und den Betrieb eines Informationssystems wie das KiSS – wobei aus grundrechtlicher Sicht und auf der Grundlage des Gesetzmässigkeitsprinzips im Übrigen einiges dafür spricht, ein solches Informationssystem zumindest in einer materiellrechtlichen Grundlage zu verankern – anwendbaren **rechtlichen Vorgaben** durchaus **konkretisierbare Anforderungen** in Bezug auf die **Zugangsrechte** entnommen werden können. Es unterliegt gewissen Zweifeln, ob diesen bei der Errichtung und dem Betrieb solcher Systeme in den Kantonen immer Rechnung getragen wird bzw. diesbezüglich könnten zumindest ernsthafte Fragen aufgeworfen werden. Der Grund hierfür dürfte wohl weniger darin zu sehen sein, dass die verantwortlichen Behörden datenschutzrechtliche

---

97 C.IV.
98 C.V.
99 C.V.3.

Vorgaben nicht berücksichtigen wollten, denn darin, dass die zu beachtenden Anforderungen nach Art. 6 lit. b KDSG bzw. den entsprechenden Bestimmungen in anderen Kantonen – wonach eben vorausgesetzt wird, dass die Bearbeitung besonders schützenswerter Personendaten **zwingend für die Erfüllung der gesetzlichen Aufgabe erforderlich** ist – über die „normalen" Anforderungen der Verhältnismässigkeit insbesondere insofern hinausgehen, als Gesichtspunkte der Verwaltungseffizienz – von Ausnahmen allenfalls abgesehen – grundsätzlich nicht ausreichen, um eine bestimmte Datenbearbeitung zu begründen. Im Übrigen implizieren die erörterten datenschutzrechtlichen Anforderungen, dass eine Organisations- und Verwaltungsstruktur gewählt wird, die diesen Vorgaben Rechnung zu tragen vermag. M.a.W. muss sich vor dem Hintergrund der hohen grundrechtlichen Relevanz der Bearbeitung besonders schützenswerter Personendaten die **Verwaltungsorganisation an die Anforderungen des Datenschutzes anpassen (und nicht umgekehrt)**.

Es ist nicht zu verkennen, dass hiermit **Effizienzverluste** bzw. ein höherer Aufwand für die Verwaltung einhergehen kann und häufig auch wird. So wird Datenschutz denn auch häufig als „Effizienzhindernis" für die Wahrnehmung bestimmter (öffentlicher) Aufgaben angesehen. Diese Feststellung ist durchaus im Grundsatz zutreffend, wäre es doch für die Behörden am effizientesten, wenn möglichst viele Daten der Bürger und Bürgerinnen bei ihnen vorhanden und möglichst schrankenlos zugänglich wären und ausgetauscht werden könnten. In einem **Rechtsstaat** darf jedoch Effizienz grundsätzlich kein Grund dafür sein, wesentlich eingestufte Errungenschaften eben dieses Rechtsstaats „ausser Kraft zu setzen". Vielmehr ist der Rechtsstaat an sich teilweise (zumindest zunächst) ineffizient; man denke etwa – über die in diesem Beitrag angesprochenen Fragen hinaus – an die Vorgaben für ein faires Verfahren oder an die durch die Polizei zu beachtenden Vorschriften. Nur am Rande sei in diesem Zusammenhang bemerkt, dass der zunächst und zumindest teilweise nur anscheinend bestehende „Gewinn" an Effizienz durch Abstriche bei der Beachtung rechtsstaatlicher Grundsätze sich durchaus zumindest mittelfristig in das Gegenteil verkehren kann, „profitiert" der Staat doch von der Akzeptanz, die einem demokratischen Rechtsstaat seitens der Bürgerinnen und Bürger entgegen gebracht wird. Insofern lohnt es sich, die Anstrengungen und den Aufwand auf sich zu nehmen, um einen über jeden (rechtlichen) Zweifel erhabenen Standard an Datenschutz und damit

an Grundrechtsschutz zu gewährleisten, zumal es die erörterten Garantien durchaus erlauben, die in Frage stehenden öffentlichen Interessen zu verfolgen.

E. Literatur

Baeriswyl, Bruno: Entwicklungen und Perspektiven des Datenschutzes in öffentlich-rechtlichen Krankenhäusern – Erfahrungen aus dem Kanton Zürich, in: Hürlimann, Barbara/Jacobs, Reto/Poledna, Thomas (Hrsg.), Datenschutz im Gesundheitswesen, Zürich 2001, 49 ff.

Belser, Eva Maria/Epiney, Astrid/Waldmann, Bernhard: Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011 (zitiert: *Verfasser*, in: Belser/Epiney/Waldmann, Datenschutzrecht).

Bondallaz, Stéphane: La protection des personnes et de leurs données dans les télécommunications, Zürich 2007.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB): Technische und organisatorische Massnahmen, ein Leitfaden, September 2011.

Epiney, Astrid: Zu ausgewählten Herausforderungen des Datenschutzrechts, in: Astrid Epiney/Sarah Theuerkauf (Hrsg.), Datenschutz in Europa und die Schweiz / La protection des données en Europe et la Suisse, Zürich 2006, 1 ff.

Epiney, Astrid: Datenschutzrechtliche Rahmenbedingungen – Zu den datenschutzrechtlichen Vorgaben für öffentliche Organe des Bundes und der Kantone, in: Schweizerische Vereinigung für Verwaltungsorganisationsrecht (Hrsg.), Verwaltungsorganisationsrecht – Staatshaftungsrecht – öffentliches Dienstrecht. Jahrbuch 2010, Bern 2011, 5 ff.

Epiney, Astrid/Civitella, Tamara/Zbinden, Patricia: Datenschutzrecht in der Schweiz. Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, Freiburger Schriften zum Europarecht Nr. 10, Freiburg 2009.

Epiney, Astrid/Schleiss, Yvonne, Ausgewählte Aspekte des Art. 19 Abs. 3 DSG (Abrufverfahren), Jusletter vom 7. November 2011.

Gächter, Thomas/Egli, Philipp: Informationsaustausch im Umfeld der Sozialhilfe, Jusletter vom 6. September 2010.

Maurer-Lambrou, Urs/Vogt, Nedim Peter (Hrsg.): Datenschutzgesetz, Basler Kommentar, 2. Aufl., Basel 2006 (zitiert: *Verfasser*, in: Mauer-Lambrou/Vogt, BK Datenschutzgesetz).

Meier, Philippe: Protection des données, Fondements, principes généraux et droit privé, Bern 2011.

Mösch Payot, Peter: Datenschutz im Sozialbereich: Aktuelle Herausforderungen, in: Kieser, Ueli/Pärli, Kurt (Hrsg.), Datenschutz im Arbeits-, Versicherungs- und Sozialbereich: Aktuelle Herausforderungen, St. Gallen 2012, 109 ff.

Rosch, Daniel: SPECIAL Workshop: Menschenrechte und Datenschutz in der Sozialen Arbeit, in: Kirchschläger, Peter/Kirchschläger, Thomas (Hrsg.), Menschenrechte und Digitalisierung des Alltags, 7. Internationales Menschenrechtsforum Luzern (IHRF) 2010, Bern 2010, 261 ff.

Rosenthal, David/Jöhri, Yvonne: Handkommentar zum Datenschutzgesetz, sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zitiert: *Verfasser*, in: Rosenthal/Jöhri, Handkommentar DSG).

Schwegler, Ivo: Datenschutzrecht, in: Müller, Markus/Feller, Reto (Hrsg.), Bernisches Verwaltungsrecht, Bern 2008, 6. Kapitel, 307 ff.

Schweizer, Alex: Data Mining, Data Warehouse, Zürich 1999.

Uttinger, Ursula: Datenschutz in der Krankenversicherung, insbesondere im vertrauensärztlichen Dienst, HAVE 2007, 253 ff.

Weber, Rolf H.: Datenschutzrecht vor neuen Herausforderungen. Marketing – E-Commerce – Virtuelle Bank – Sachdaten, Zürich 2000.

Wermelinger, Amédéo/Schweri, Daniel: Teilrevision des Eidgenössischen Datenschutzrechts – Es nützt nicht viel, schadet es etwas?, Jusletter v. 3.3.2008.

Zehnder, Carl-August: Datenschutz aus der Sicht eines Informatikers – seit es Datenbanken gibt, in: Datenschutz-Forum Schweiz (Hrsg.), Von der Lochkarte zum Mobile Computing. 20 Jahre Datenschutz in der Schweiz, Zürich 2012, 147 ff.

F. Abkürzungen

a.A.	anderer Ansicht
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
Art.	Artikel
Bd.	Band
BGE	Bundesgerichtsentscheid
BGer	Bundesgericht
B-Modul	Basis-Modul
BSG	Bernische Systematische Gesetzessammlung
bspw.	beispielsweise
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101
bzw.	beziehungsweise
ca.	circa
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR 235.1
DSK	Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1
DSV	Datenschutzverordnung vom 22. Oktober 2008, BSG 152.040.1
E.	Erwägung
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EGMR	Europäischer Gerichtshof für Menschenrechte
EKS	Amt für Erwachsenen- und Kindesschutz der Stadt Bern
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, SR 0.101
f./ff.	folgende/und folgende
F-Modul	Fallführungs-Modul
Fn.	Fussnote
ggf.	gegebenenfalls

i.e.S.	im engeren Sinne
i.S.v.	im Sinne von
IG	Gesetz über die Information der Bevölkerung vom 2.11.1993, BSG 107.1
I-Modul	Inkasso-Modul
KDSG	Datenschutzgesetz vom 19. Februar 1986, BSG 152.04
KESB	Kindes- und Erwachsenenschutzbehörde des Kantons Bern
KESG	Gesetz über den Kindes- und Erwachsenenschutz vom 1. Februar 2012, BSG 213.316
KESV	Verordnung über den Kindes- und Erwachsenenschutz vom 24. Oktober 2012, BSG 213.316.1
KiSS	Klienten-Informationssystem für Sozialarbeit
KV-BE	Verfassung des Kantons Bern vom 6. Juni 1993, BSG 101.1
lit.	litera
m.a.W.	mit anderen Worten
m.w.N.	mit weiteren Nachweisen
Nr.	Nummer
o.ä.	oder ähnliche
OV	Verordnung über die Organisation der Stadtverwaltung vom 27. Februar 2001, SSSB 152.01
RL 95/46	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281, 31 ff.
Rn.	Randnummer
s.	siehe
s.o.	siehe oben
SHG	Gesetz über die öffentliche Sozialhilfe vom 11. Juni 2001, BSG 860.1

SHV	Verordnung über die öffentliche Sozialhilfe (SHV) vom 24. Oktober 2001, BSG 860.111
S-Modul	Sozialhilfe-Modul
sog.	sogenannte(n)
SR	Systematische Sammlung des Bundesrechts
SSSB	Systematische Sammlung des Stadtrechts von Bern
u.a.m.	und andere mehr
u.E.	unseres Erachtens
Urt.	Urteil
usw.	und so weiter
v.	vom
VDSG	Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz, SR 235.11
vgl.	vergleiche
V-Modul	Vormundschafts-Modul
z.B.	zum Beispiel
ZAV	Verordnung über die Zusammenarbeit der kommunalen Dienste mit den Kindes- und Erwachsenenschutzbehörden und die Abgeltung der den Gemeinden anfallenden Aufwendungen vom 19. September 2012, BSG 213.318
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210
Ziff.	Ziffer